

319-CD-003-003

## **EOSDIS Core System Project**

# **CSMS Integration and Test Plan for the ECS Project Volume 1: IR-1**

Final

June 1995

Hughes Information Technology Corporation  
Landover, Maryland

# **CSMS Integration and Test Plan for the ECS Project Volume 1: IR-1**

**June 1995**

Prepared Under Contract NAS5-60000  
CDRL Item 054

## **SUBMITTED BY**

<u>E. M. Lerner /s/</u>	<u>6/30/95</u>
Ed Lerner, CSMS Segment Manager	Date
EOSDIS Core System Project	

**Hughes Information Technology Corporation**  
Landover, Maryland

This page intentionally left blank.

# Preface

---

This document is a formal contract deliverable with an approval code 1. It requires Government review and approval prior to acceptance and use. Documents with approval code 1 are formal contract deliverables which require Government review and approval prior to their acceptance and use. This document is under ECS Contractor Configuration Control. Once this document is approved, Contractor-approved changes are handled in accordance with Class I and Class II change control requirements described in the EOS Configuration Management Plan. Changes to this document shall be made by document change notice (DCN) or by complete revision.

Any questions should be addressed to:

Data Management Office  
The ECS Project Office  
Hughes Information Technology Corporation  
1616 McCormick Dr.  
Landover, MD 20785

This page intentionally left blank.

# Abstract

---

This document specifies the Test Plan (IR-1) for the Communications and Systems Management Segment (CSMS) of the ECS Project. It includes descriptions of: the CSMS test methodology, Build/Thread functional decomposition, detailed test cases, requirements traceability matrices between Level 4 requirements and test cases, and descriptions of resources and test tools needed for these tests. The information provided in this plan will serve as a baseline for developing the follow-on test procedures (DID 322).

**Keywords:** Integration, Test, I&T, Build, Thread, Interim Release One (IR-1), CSMS, traceability, Level 4, test case(s), requirements, test tools

This page intentionally left blank.

# Change Information Page

List of Effective Pages			
Page Number		Issue	
Title		Final	
iii through xiv		Final	
1-1 and 1-2		Final	
2-1 and 2-2		Final	
3-1 through 3-12		Final	
4-1 through 4-66		Final	
A-1 and A-2		Final	
B-1 through B-22		Final	
C-1 and C-4		Final	
AB-1 through AB-4		Final	
Document History			
Document Number	Status/Issue	Publication Date	CCR Number
319-CD-003-001	Review Copy	December 1994	
319-CD-003-002	Final	March 1995	95-0145
319-CD-003-003	Update	June 1995	95-0456

This page intentionally left blank.

# Contents

---

## Preface

## Abstract

## 1. Introduction

1.1	Identification .....	1-1
1.2	Scope .....	1-1
1.3	Purpose .....	1-1
1.4	Status and Schedule .....	1-1
1.5	Organization .....	1-2

## 2. Related Documentation

2.1	Parent Documents .....	2-1
2.2	Applicable Documents .....	2-1
2.3	Information Documents .....	2-2
2.3.1	Information Documents Referenced .....	2-2
2.3.2	Information Documents Not Referenced .....	2-2

## 3. CSMS Integration and Test Organization Overview

3.1	CSMS I&T Organization and the ECS Environment .....	3-1
3.1.1	CSMS Functional Overview .....	3-1
3.1.2	CSMS I&T Organization Relationship to other Test Groups .....	3-2
3.2	CSMS I&T Organization Testing Approach .....	3-4
3.2.1	Segment I&T Functional Testing .....	3-4
3.2.2	CSMS Build/Thread Methodology .....	3-4
3.3	CSMS I&T Organization Test Verification .....	3-5

3.3.1	Verification Methods .....	3-5
3.3.2	Post Test Analysis .....	3-6
3.3.3	Regression Testing .....	3-6
3.3.4	Verification Resources .....	3-7
3.4	CSMS I&T Organizations Roles and Responsibilities .....	3-9
3.5	CSMS I&T Release Testing .....	3-10
3.6	CSMS I&T Schedule Overview .....	3-10
3.6.1	Release Schedule .....	3-10
3.6.2	CSMS I&T Schedule for IR-1 .....	3-12

## 4. IR-1 Test Descriptions

4.1	DCE Infrastructure Thread Test .....	4-1
4.1.1	Test Case 1.1: User Authentication (TC003.001) .....	4-1
4.1.2	Test Case 1.2: Failed User Authentication (TC003.002) .....	4-2
4.1.3	Test Case 1.3: User Password Change (TC003.003) .....	4-3
4.1.4	Test Case 1.4: User Password Reset (TC003.004) .....	4-4
4.1.5	Test Case 1.5: Security Registry Maintenance (TC003.005) .....	4-5
4.1.6	Test Case 1.6: Security Privilege Test (TC003.006) .....	4-6
4.1.7	Test Case 1.7: Server Authentication (TC003.007) .....	4-6
4.1.8	Test Case 1.8: Authentication Expiration (TC003.008) .....	4-7
4.1.9	Test Case 1.9: Local Logons (rlogin) - Valid and Invalid (B01.01.01) .....	4-8
4.1.10	Test Case 1.10: Remote Logons (Telnet H1-H2-H3) - Valid and Invalid (B01.01.02) .....	4-9
4.1.11	Test Case 1.11: Remote Logons (Telnet H1-H3-H1) - Valid and Invalid (B01.01.03) .....	4-9
4.1.12	Test Case 1.12: Syntax and Commands Simplification (TC011.001) .....	4-10
4.1.13	Test Case 1.13: Sample Object Implementation (TC011.002) .....	4-11
4.2	Messaging and File Transfer Thread Test .....	4-14
4.2.1	Test Case 2.1: Internet Utilities Test (TS002.014) .....	4-14
4.2.2	Test Case 2.2: Bulletin Board (BC012.004) .....	4-15
4.2.3	Test Case 2.3: E-Mail (TC006.002) .....	4-17
4.2.4	Test Case 2.4: EDF to DAAC Message Transfer (TC010.001) .....	4-18
4.2.5	Test Case 2.5: E-Mail from EDF to GSFC (T01-02.05.01) .....	4-19
4.2.6	Test Case 2.6: E-Mail from EDF to LaRC (T01-02.05.02) .....	4-19

4.2.7	Test Case 2.7: SCF to DAAC Message Transfer (TC010.002) .....	4-20
4.2.8	Test Case 2.8: E-Mail from EDF to EDC (T01-02.05.04) .....	4-21
4.2.9	Test Case 2.9: DAAC to DAAC Message Transfer (TC010.003) .....	4-21
4.2.10	Test Case 2.10: E-Mail from DAAC to DAAC (T01-02.05.05) .....	4-22
4.2.11	Test Case 2.11: E-Mail- Asynchronous Messaging (TC006.001) .....	4-23
4.2.12	Test Case 2.12: Sending E-Mail Messages to Local and Remote Hosts (B01.05.01) .....	4-24
4.2.13	Test Case 2.13: Receiving E-Mail Messages to Local and Remote Hosts (B01.05.02) .....	4-24
4.2.14	Test Case 2.14: Client/User File Transfer (TC009.001) .....	4-25
4.2.15	Test Case 2.15: Transmit File from EDF to GSFC (ftp) (T01-02.04.01) .....	4-26
4.2.16	Test Case 2.16: Transmit File from EDF to LaRC (ftp) (T01-02.04.02) .....	4-26
4.2.17	Test Case 2.17: Transmit File from EDF to MSFC (ftp) (T01-02.04.03) .....	4-27
4.2.18	Test Case 2.18: Transmit File from EDF to EDC (ftp) (T01-02.04.04) .....	4-27
4.2.19	Test Case 2.19: Transmit File from EDF to GSFC (rcp) (T01-02.04.05) .....	4-28
4.2.20	Test Case 2.20: Transmit File from EDF to LaRC (rcp) (T01-02.04.06) .....	4-29
4.2.21	Test Case 2.21: Transmit File from EDF to MSFC (rcp) (T01-02.04.07) .....	4-29
4.2.22	Test Case 2.22: Transmit File from EDF to EDC (rcp) (T01-02.04.08) .....	4-30
4.2.23	Test Case 2.23: Anonymous ftp (TC009.003) .....	4-30
4.2.24	Test Case 2.24: Application File Transfer (TC009.004) .....	4-31
4.2.25	Test Case 2.25: Network Filtering Test (BC002.003) .....	4-32
4.2.26	Test Case 2.26: Multiple Accounts Transmitting Large Data Files to GSFC DAAC (B01.07.01) .....	4-32
4.2.27	Test Case 2.27: Multiple Accounts Transmitting Large Data Files Within the EDF (B01.07.02) .....	4-33
4.2.28	Test Case 2.28: External Interfaces Integration Test (BC002.001) .....	4-34
4.3	System Management Thread Test .....	4-37
4.3.1	Test Case 3.1: X/Open Functions (TC004.001) .....	4-38
4.3.2	Test Case 3.2: Replication (TC004.002) .....	4-38
4.3.3	Test Case 3.3: Distribution (TC004.003) .....	4-39
4.3.4	Test Case 3.4: Single Host Time Synchronization (TC005.001) .....	4-40
4.3.5	Test Case 3.5: Multiple Host Time Synchronization (TC005.002) .....	4-41
4.3.6	Test Case 3.6: Inaccuracy Injection (TC005.003) .....	4-43
4.3.7	Test Case 3.7: DTS Management (TC005.004) .....	4-43
4.3.8	Test Case 3.8: DTS Security (TC005.005) .....	4-45

4.3.9	Test Case 3.9: DBMS Interface (TC013.003).....	4-45
4.3.10	Test Case 3.10: Management Data Access (TC013.004) .....	4-47
4.3.11	Test Case 3.11: Performance Monitoring Thresholds (TC013.005).....	4-48
4.3.12	Test Case 3.12: Basic Monitoring (TC014.001) .....	4-50
4.3.13	Test Case 3.13: OpenView (TC014.002).....	4-51
4.3.14	Test Case 3.14: Fault Indication (TC014.003).....	4-53
4.3.15	Test Case 3.15: MUI Services (TC014.004).....	4-54
4.3.16	Test Case 3.16: Performance Management (TC014.005).....	4-55
4.3.17	Test Case 3.17: Monitor/Control and Management Agent (TC014.006) .....	4-56
4.3.18	Test Case 3.18: Problem Tracking Test (TS002.011).....	4-57
4.3.19	Test Case 3.19: Remote NCR (BC016.003) .....	4-57
4.3.20	Test Case 3.20: Hardware Monitoring Process Terminated (T04-01.01.06) .....	4-58
4.3.21	Test Case 3.21: Gateway/Router Monitoring Process Terminated.....	4-58
4.3.22	Test Case 3.22: Software Application Monitoring Process Termination (T04-01.01.12) .....	4-59
4.3.23	Test Case 3.23: Computer Monitoring Process Terminated (T04-01.01.18) .....	4-60
4.3.24	Test Case 3.24: Operating System Monitoring Process Terminated .....	4-60
4.3.25	Test Case 3.25: Local Site Management/Security Policy and Procedures .....	4-61
4.3.26	Test Case 3.26: Active DAAC ECS Administrator Account (T04-01.05.01) .....	4-61
4.3.27	Test Case 3.27: ECS Software Backup Maintained (T04-01.05.02) .....	4-62
4.3.28	Test Case 3.28: Monitoring and Replenishment of Spares Inventory .....	4-62
4.4	System Administration Build Test .....	4-63
4.4.1	Test Case 4.1: General DCE (BC008.001) .....	4-63
4.4.2	Test Case 4.2: Network Management Test (BC002.004) .....	4-64
4.4.3	Test Case 4.3: Fault Management (T04-01.02.01) .....	4-65
4.4.4	Test Case 4.4: Security Management (T04-01.02.02) .....	4-65
4.4.5	Test Case 4.5: Access to GSFC (T01-02.02.02) .....	4-66
4.4.6	Test Case 4.6: Access to LaRC (T01-02.02.03) .....	4-66
4.4.7	Test Case 4.7: Access to MSFC (T01-02.02.04) .....	4-67
4.4.8	Test Case 4.8: Internetworking Test (BC002.002) .....	4-67

## Figures

3.2-1	Interim Release One Build/Thread Diagram .....	3-5
4.2-1	Interim Release One DEC Cell Topology.....	4-34
4.2-2	Interim Release One External Interfaces .....	4-35

## Tables

3.1-1.	CSMS IR-1 CIs .....	3-1
3.6-1.	CSMS I&T Release Schedule .....	3-11

## Appendix A. Test Tool Descriptions

## Appendix B. Verification Traceability Matrix

## Abbreviations and Acronyms

This page intentionally left blank.

# 1. Introduction

---

## 1.1 Identification

This document is submitted as required by CDRL item 054, DID 319/DV1 whose requirements are specified as a required deliverable under the Earth Observing System (EOS) Data and Information System (EOSDIS) Core System (ECS), Contract (NAS5-60000).

## 1.2 Scope

This document defines the plan for integration, test, and verification of the Communications and System Management Segment, referred to as CSMS, for each Release. There is a separate document for each proceeding release. It is one of three segment test plans (per release) required to test ECS at the segment level. There is a separate test plan for the Flight Operations Segment (FOS) and the Systems and Data Processing Segment (SDPS). The CSMS Integration and Test Plan applies only to segment and element level verification activities. This plan includes verifying that the ECS complies with the CSMS Level 4 Functional Requirements, and the ECS design specifications. The roles and activities of the Communications and System Management Segment Integration and Test Organization (CSMS I&T Organization) are described and schedules for performing CSMS I&T Organization activities are included.

This document reflects the Technical Baseline submitted via contract correspondence no. ECS 194-00343.

## 1.3 Purpose

This Segment/Element Integration and Test Plan describes the test, review, and analysis effort to be conducted by the CSMS I&T organization for CSMS Segment/Element for Interim Release One (IR-1). This document presents the overall processes and activities associated with verifying the CSMS Segment/Element during the segment integration and test phase of the CSMS development. This test plan provides an outline of the activities to be performed for CSMS I&T, and is later used to prepare test procedures which provide more detailed instructions for verification of the CSMS software. It delineates the roles and responsibilities of each organization associated with the segment integration and test activities.

## 1.4 Status and Schedule

The EOSDIS Core System, Contract Data Requirements Document specifies the Segment/Element Integration and Test Plan (DID # 319/DV1) is delivered two weeks prior to each PDR and IDR. In order to support the development of CSMS software in Releases this plan is updated on an incremental delivery schedule dependent on major releases and reviews such as PDR and IDR.

As a PDR deliverable, this document discusses the CSMS I&T process which includes a Build Thread Plan for the CSMS I&T organization of its elements and subsystems for Interim Release One. The Build and Thread Tests are described at a summary level identifying test objectives, inputs, outputs, and success criteria. Test databases and test tools needed for each test are identified. Corresponding documents including tests for Release A, B, C, and D will be provided at appropriate IDRs.

This submittal of DID 319/DV1 meets the milestone specified in the Contract Data Requirements List (CDRL) of NASA Contract NAS5-60000. It is anticipated that this submittal will be reviewed during the appropriate segment- or system-level Preliminary Design Review (PDR), and that subsequent changes to the document will be incorporated into a resubmittal according to a schedule mutually agreed to by GSFC and ECS.

## **1.5 Organization**

This document, which is based on IR-1 requirements, is organized into five chapters:

Section 1	Introduction, contains the identification, scope, purpose and objectives, status and schedule, and document organization.
Section 2	Related Documents, provides a bibliography of parent, applicable and reference documents for the CSMS Segment Integration and Test Document.
Section 3	CSMS Segment Integration and Test Overview, describes the process used to integrate and test the CSMS Segment and subsystems.
Section 4	CSMS Segment Test Descriptions, describes the specific segment level thread and build tests, which will be used to verify the functionality of the CSMS Segment.
Appendix A	Contains a list and brief description of the test tools needed for CSMS Segment Integration and Test (IR-1).
Appendix B	Contains the requirements traceability matrix, mapping test cases to Level 4 requirements (IR-1).
Abbreviations and Acronyms	Contains a listing of abbreviations and acronyms used in this Document (IR-1).

## 2. Related Documentation

---

### 2.1 Parent Documents

The parent document is the document from which this CSMS Integration and Test Plan's (IR-1) scope and content are derived.

101-101-MG1-001	Project Management Plan for the EOSDIS Core System
194-107-MG1-XXX	Level 1 Master Schedule for the ECS Project
194-201-SE1-001	Systems Engineering Plan for the ECS Project
301-CD-002-003	System Implementation Plan for the ECS Project
402-CD-001-002	System Integration and Test Plan for the ECS Project, Volume 1: Interim Release 1 (IR-1), Final
402-CD-002-002	System Integration and Test Plan for the ECS Project, Volume 2: Release A, Final
194-501-PA1-001	Performance Assurance Implementation Plan for the ECS Project
423-41-01	Goddard Space Flight Center, EOSDIS Core System (ECS) Statement of Work
423-41-02	Goddard Space Flight Center, Functional and Performance Requirements Specification (F&PRS) for the Earth Observing System Data and Information System (EOSDIS) Core System (ECS)
423-41-03	Goddard Space Flight Center, EOSDIS Core System (ECS) Contract Data Requirements Document

### 2.2 Applicable Documents

The following documents are referenced within this CSMS Integration and Test Plan (IR-1), or are directly applicable, or contain policies or other directive matters that are binding upon the content of this volume. The following white papers are available on the ECS Data Handling System (EDHS); <http://edhs1.gsfc.nasa.gov/Info/pdr/440wp01info.html>

194-207-SE1-001	System Design Specification for the ECS Project
194-401-VE1-002	Verification Plan for the ECS Project, Final
409-CD-001-003	ECS Overall System Acceptance Test Plan for Release A, Final
194-415-VE1-002	Acceptance Testing Management Plan for the ECS Project, Final
307-CD-003-003	Communications and Systems Management Segment (CSMS) Release
329-CD-003-003	and Development Plan for the ECS Project

## **2.3 Information Documents**

### **2.3.1 Information Documents Referenced**

The following documents are referenced herein and, amplify or clarify the information presented in this document. These documents are not binding on the content of the ECS CSMS Integration and Test Plan (IR-1).

194-102-MG1-001	Configuration Management Plan for the ECS Project
193-103-MG3-001	Configuration Management Procedures for the ECS Project
305-CD-003-002	CSMS Design Specifications for the ECS Project

### **2.3.2 Information Documents Not Referenced**

The following documents, although not referenced herein and/or not directly applicable, do amplify or clarify the information presented in this document. These documents are not binding on the content of the CSMS Integration and Test Plan (IR-1).

104-CD-001-003	Data Management Plan for the ECS Project
193-105-MG3-001	Data Management Procedures for the ECS Project
194-219-SE1-018	Interface Requirements Document Between EOSDIS Core System (ECS) and Tropical Rainfall Measuring Mission (TRMM) Ground System

## 3. CSMS Integration and Test Organization Overview

---

This section contains an overview of the approach taken by the Communications and Systems Management Segment Integration and Test organization to ensure complete and thorough testing at the segment level. Included is information concerning the CSMS I&T environment, schedules and verification activities and responsibilities.

### 3.1 CSMS I&T Organization and the ECS Environment

#### 3.1.1 CSMS Functional Overview

ECS is comprised of three segments, each comprised of various subsystems. The three segments are the Flight Operations Segment (FOS), Science Data Processing Segment (SDPS) and Communications and Systems Management Segment (CSMS). Each of these segments are decomposed into subsystems and the subsystems are composed of CIs. This document will test the design and implementation of the CSMS CIs and their integration into ECS subsystems.

CSMS is responsible for the interconnection of users and service providers, the transfer of information between ECS components and systems management. CSMS is also responsible for supporting and providing interoperability for the Science Data Processing Segment (SDPS) and the Flight Operations Segment (FOS). CSMS contains three internal subsystems: Communications Subsystem (CSS), Internetworking Subsystem (ISS) and the Systems Management Subsystem (MSS). CSS is a collection of services that are responsible for providing flexible interoperability and information transfer between clients and servers. ISS is a layered stack of communications services corresponding to layers 1-4 of the OSI-RM. MSS is made up of a collection of applications that are responsible for the management of all ECS resources, including all SDPS, FOS, ISS and CSS components.

The CIs for CSMS at IR-1 are listed in Table 3.1-1. Included are CI names and CSMS subsystems. A short description of each CI is given following Table 3.1-1.

**Table 3.1-1. CSMS IR-1 CIs**

CI	Subsystem
Management Software CI (MCI)	MSS
Management Logistics CI (MLCI)	MSS
Management Agent CI (MACI)	MSS
Management Hardware CI (MHCI)	MSS
Distributed Computing Software CI (DCCI)	CSS
Distributed Communications Hardware CI (DCHCI)	CSS
Internetworking CI (INCI)	ISS
Internetworking Hardware CI (INHCI)	ISS

Management Software CI (MCI) The Management Software CI includes both Enterprise System Monitor and Local System Manager Configurations.

Management Logistics CI (MLCI) The Management Logistics CI includes both the managing of the Enterprise Logistics Manager and Domain Logistics Manager Configurations.

Management Agent CI (MACI) The Management Agent CI includes the agent specialization. An agent is the interface to a managed object. An agent system is a device, which has the responsibility of performing network management operations requested by the manager.

Management Hardware CI (MHCI) The Management Hardware CI includes: local management of ECS sites, shared workstation and server pool for enterprise and domain managers, as well as enterprise-wide (ECS-wide) monitoring and coordination.

Distributed Computing Software CI (DCCI) The Distributed Computing Software CI includes the client and server configurations. This CI includes the DCE COTS package, which is the baseline distributed computing technology chosen through Release B.

Distributed Communications Hardware CI (DCHCI) The Distributed Communications Hardware CI includes the communications servers, such as; E-mail server, directory server, security server, time server, trader server and bulletin board (user registration/toolkit distribution) server.

Internetworking CI (INCI) The Internetworking CI includes the COTS implementations of the communication protocols reserved by network nodes. This includes protocols and standards for layer four and below of the OSI/ISO reference model (e.g., TCP, IP, OSPF, RIP).

Internetworking Hardware CI (INHCI) The Internetworking Hardware CI includes all COTS network devices and cabling: routers, hubs, switches, and test equipment. It does not include host interface cards.

### **3.1.2 CSMS I&T Organization Relationship to other Test Groups**

The CSMS I&T organization is responsible for integration and test at the subsystem level. This includes acceptance of software components upon completion of unit testing, integration of these components into segment subsystems, complete and thorough testing of the integrated software, and recording and reporting of any problems encountered during testing. Integrated software units are tested against Level 4 requirements documented in the Segment/Element Requirements Specification (ECS document number 304-CD-003-001). The CSMS I&T organization is responsible for verifying functional components and intra-segment interfaces. When necessary, the interfaces will be simulated.

The CSMS I&T organization interacts with and supports other ECS and independent test organizations. This includes the Quality Office, Systems Integration and Test, the Independent Acceptance Test Organization (IATO), and EOSDIS Independent Verification and Validation (IV&V) Contractor. The IATO monitors segment tests and identifies any Level 3 requirements that can be verified through analysis of segment test results. The IV&V contractor monitors ECS verification activities.

The Quality Office assists in identifying training needs of test personnel and schedules formal training. The Quality Office conducts requirements traceability audits during the Implementation and Integration and Test phases as each test case is completed and evaluated. They are responsible for monitoring the hardware inspection and unit-level verification procedures and verify segment and system test plans for completeness. They also validate segment and system integration and tests and test results. The Quality Office participates in segment test implementation, reviews, and analysis. They are also responsible for monitoring the life cycle of the nonconformance reports and participating in the final decision on product acceptability.

Upon completion of CSMS testing, the software is delivered to the ECS System I&T organization. This group is responsible for integration and test of the CSMS and SDPS deliverables at the system level. This includes verification of all SDPS, and CSMS segment software. The System I&T organization starts with the highest level builds at the segment level and uses them as system threads for tests. These threads are then combined into system level builds and tested. The system builds may include system threads derived from different segments. These builds are aggregated with other system threads (previously tested) and/or other tested builds, which are also tested. This process is repeated for all of the system builds until the entire release is integrated and tested. Testing is done to confirm compliance to Level 3 requirements documented in the Functional and Performance Requirements Specification (Goddard document number 423-41-02) and the System Design Specification (ECS document number 194-207-SE1-001). Internal interfaces are tested with ECS software and hardware where available. Informal verification of the external interfaces is accomplished during the Systems I&T phase using simulators or locally devised tests to reduce the risk of acceptance testing with immature external interfaces.

The Independent Acceptance Test Organization (IATO) is provided with the system level builds upon completion of testing by the Systems I&T Organization. Acceptance testing involves preparation at the EDF prior to CSR (Consent to Ship Review), and formal testing at the operational centers after CSR. Testing at the operational centers provides the IATO an opportunity to test using the unique operational configuration of each operational center. By testing on site and emphasizing science and operational scenarios, acceptance testing will be functioning in more of a "real-world" environment than the previous levels of testing. Most Level 3 requirements will be verified through formal release acceptance testing at ECS centers. However, to alleviate some of the work that is involved in release acceptance testing at the ECS centers, some level 3 requirements will be verified at the acceptance level by analyzing the results of the segment and systems I&T at the EDF. This will only occur for requirements that can be satisfied by inspecting the results of the segment and system I&T test results.

Upon completion of the RRR (Release Readiness Review), the Independent Verification and Validation (IV&V) contractor provides an independent assessment of the functionality and performance of ECS releases. The IV&V contractor is responsible for pre-operational testing performed at the ECS centers and the validation of the ECS Level 3 requirements. They are also responsible for the reporting and tracking of nonconformances identified during this phase of testing. The IATO, which serves as the ECS contractor's primary contact for the IV&V contractor, supports the IV&V test team at the ECS centers. The IV&V contractor has access to all ECS contractor test activities and technical information. The IATO coordinates the resources required for testing by the IV&V contractor at each of the ECS centers.

## **3.2 CSMS I&T Organization Testing Approach**

The CSMS I&T organization will integrate and verify CSMS CI functionality on an incremental basis. As incremental integration and testing proceeds, larger portions of the segment are assembled.

### **3.2.1 Segment I&T Functional Testing**

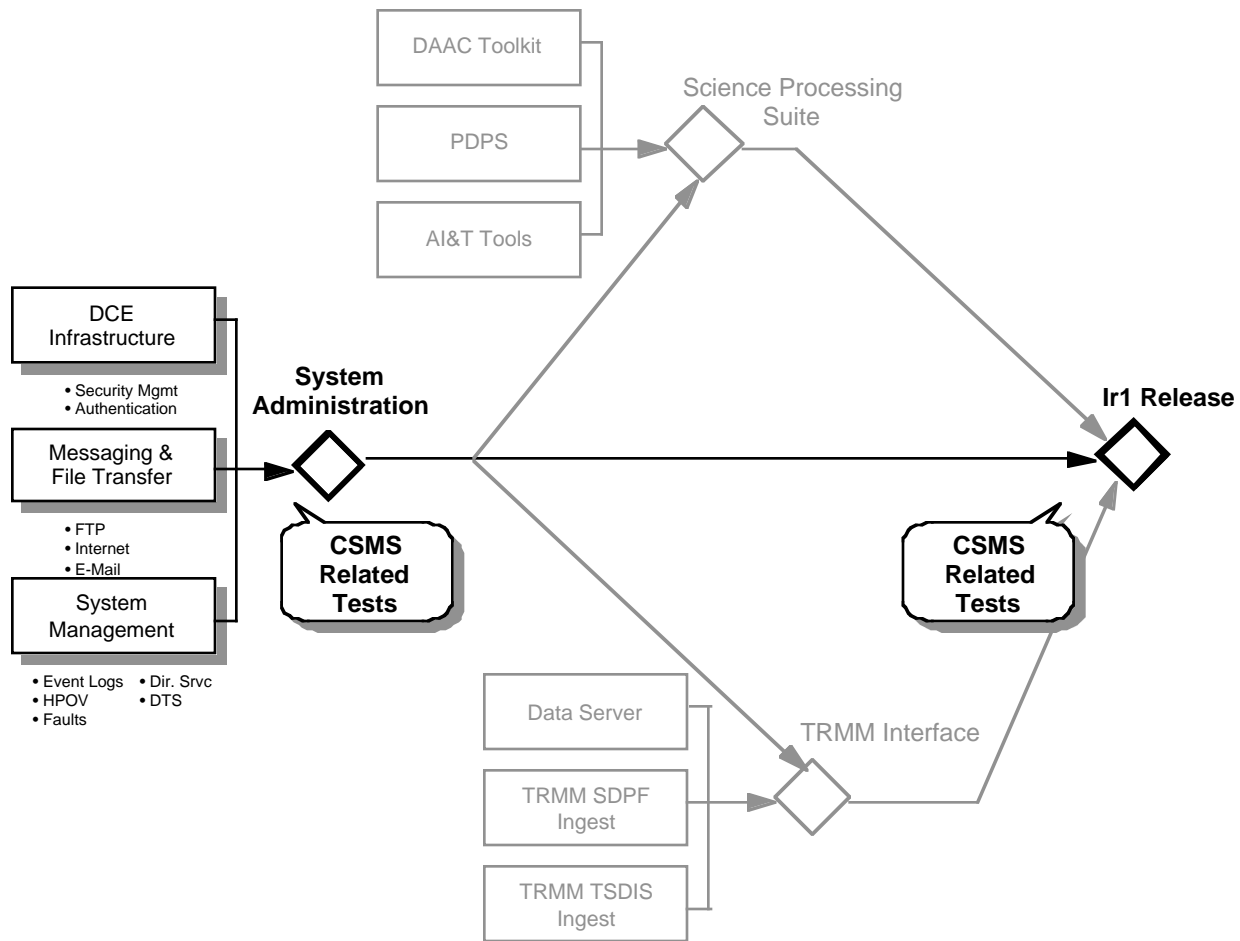
As unit testing on software and hardware items is completed unit testing, the CSMS I&T organization incrementally assembles lower-level functionality into progressively higher levels until ultimately a segment is completely integrated and tested. Functional components that are integrated are threads, and the result of combining threads is a build. Functional testing verifies Level 4 functional requirements.

### **3.2.2 CSMS Build/Thread Methodology**

The build/thread concept, which is based on the incremental aggregation of functions, is used to plan CSMS I&T activities. A CSMS thread is the set of components (software CIs, hardware and data) and operational procedures that implement a function or set of related functions at the segment level. Threads are tested individually to facilitate Level 4 requirements verification and to isolate software problems. A build is an assemblage of threads to produce a gradual buildup of segment capabilities. This orderly progression of combining lower level software and/or hardware items to form higher level items with broader capability is the basis of CSMS integration. The build tests are generally regression tests of the threads and/or builds that make up the build. CSMS builds are combined with other CSMS builds and threads to produce higher level builds. Verification of threads and builds is accomplished at progressively higher levels as the CSMS software is assembled for each release.

CSMS build/thread diagrams are developed for each release. The build/thread diagram for IR-1 is presented in Figure 3.2-1. Threads and builds are defined by examining CSMS CIs, Level 4 requirements and segment/element design specifications. The CSMS I&T organization, with support from the CSMS development community, logically groups the CSMS release into functional categories divided along noticeable boundaries. These categories are the basis for CSMS threads. Threads are combined to define CSMS builds. Builds include several integrated thread functions. The build/thread diagram for each CSMS release acts as a framework for development of CSMS test case definition. From each build and thread on the diagram, test cases are developed. These test cases provide the basis for development of step-by-step test instructions to be documented as CSMS test procedures.

The CSMS build/thread diagrams and other ECS segment level diagrams (FOS and SDPS), are combined to create a foundation for the build/thread diagrams developed for system level testing (ECS System Integration & Test Plan). CSMS and other segment build/thread testing provides an approach for first-level testing and validation of component functionality at the segment level. System I&T combines segment level build/threads into a system release which validates ECS design against Level 3 requirements and user needs.



**Figure 3.2-1. Interim Release One Build/Thread Diagram**

### 3.3 CSMS I&T Organization Test Verification

The following sections define responsibilities and activities of the CSMS I&T organization. CSMS I&T verification includes definition of verification methods, post test analysis, regression testing, and verification resources.

#### 3.3.1 Verification Methods

The four verification methods used for CSMS I&T activities include: inspection, analysis, demonstration, and test.

As defined in the ECS Verification Plan (Contract # 194-401-VE1-002).

- a. Inspection. The visual, manual examination of the verification item and comparison to the applicable requirement or other compliance documentation, such as engineering drawings.

- b. Analysis. Technical or mathematical evaluation based on calculation, interpolation, or other analytical methods.
- c. Demonstration. Observation of the functional operation of the verification item in a controlled environment to yield qualitative results without the use of elaborate instrumentation or special test equipment.
- d. Test. A procedure or action taken to determine under real or simulated conditions the capabilities, limitations, characteristics, effectiveness, reliability, or suitability of a material, device, system, or method.

Each segment level requirement will be tested and verified by one or more of these methods. A requirements matrix, mapping test cases to level 4 requirements, will include the method of verification. This matrix, mapping IR-1 segment level requirements to IR-1 test cases, is provided in Appendix B of this document.

### **3.3.2 Post Test Analysis**

Post-test analysis includes data reduction and comparison of actual results against expected results. Any post test analysis required for CSMS I&T activities will be performed by the CSMS I&T organization with support from the user and development communities when appropriate. Methods for performing post-test analysis will be documented in the Segment/Element Integration and Test Procedures on a test by test basis. Post-test analysis will be documented in CSMS I&T activities reports. Data, data logs, event logs and any other test output required for post test analysis will be captured and stored under CM control.

### **3.3.3 Regression Testing**

Regression testing is supplemental testing performed at any time upon any build or thread during CSMS I&T testing to ensure that existing software is not adversely affected by modified or new software. CSMS I&T organization is responsible for planning, documenting, executing and reporting all regression testing. Automated test tools are used, when practical, for regression testing by the CSMS I&T organization. This ensures that regression tests duplicate initial test procedures.

IR-1 Regression Testing will occur as a result of:

- software changes
- hardware changes
- operational enhancements
- integration of two or more builds
- new versions delivered after unit level testing

CSMS I&T organization is responsible for reporting any discrepancies encountered during segment regression testing. Discrepancies resulting from any other level of testing (i.e. System Test, Acceptance Test) which results in modification at the unit level, will be regression tested at the segment level by the CSMS I&T organization.

### **3.3.4 Verification Resources**

The following paragraphs in this section introduce and identify the resources necessary to accomplish CSMS I&T activities. Included are identification of test location and hardware and software configurations. Also discussed are the use of automated test tools, discrepancy reporting, and the role of CM in CSMS I&T activities.

#### **3.3.4.1 Testing Facilities**

The ECS Development Facility (EDF), located at the ECS facility in Landover , Md., has been designated as the testing facility for CSMS I&T activities. All CSMS segment level test activities will take place at this location. This facility will be shared by the Segment Integration and Test personnel, Systems Integration and Test organization, the Independent Acceptance Test Organization and some developers. The test facility will be set up to emulate a DAAC or the EOC and will be re configurable to emulate the different functionality at each of the relevant DAACs. The facility will also have the capability to replicate, as close as possible, the interfaces that will exist in IR-1 (e.g., DAAC to DAAC, SCF to DAAC, etc.). ECS will be solely responsible for the test environment. This includes installation, initial checkout and startup, upgrades/version control, access control, and maintenance.

##### **3.3.4.1.1 Hardware Items**

The hardware CIs available for the IR-1 time frame will be configured, as closely as possible (with the available EDF I&T hardware ) to emulate the various DAACs and the EOC. The hardware will also be used to emulate all communications interfaces available for IR-1, as closely as possible.

##### **3.3.4.1.2 Software Items**

For a complete listing of CSCIs mapped to test cases, please see Appendix C.

#### **3.3.4.2 Test Tools and Test Data**

The CSMS I&T organization uses test tools for test development, test execution, and test management. Whenever possible, test tools from the unit development and unit test environments are used. Additional test tools are COTS products or are developed by the Segment I&T organization. For a complete listing and description of the test tools please see Appendix A. All test cases which require an interface with SCF, ADC and user interfaces will be simulated. In all cases where testing of the DAACs is mentioned, we are referring to the ECS deployed facilities.

During CSMS test development, test tools will be used to develop test scripts and map requirements to test cases. The CSMS I&T organization will use the ECS selected tools for test script development and requirements traceability. The ECS selected capture/playback tools will be used to aid in the development of test procedures. The ECS selected Requirements & Traceability Management (RTM) tool to be used for mapping CSMS I&T test cases to level 4 requirements. This tool is used for all releases. A unique number is assigned to each

build/thread and test case. This number is then used to identify the build/thread test case in RTM. The format for this identification number is consistent throughout all test organizations within ECS. The format is (B/T), for build or thread, (S/C/F/X/A), S - SDPF, C - CSMS, F - FOS, X - SI&T and I - IATO, (xxx) - representing the build/thread number and (xxx) representing the test case number within that build (e.g., BC001.001).

During CSMS test execution, test tools will be used to simulate data and interfaces, decipher and monitor the data transmitted over the network and facilitate the execution of test procedures. Data interface simulators and user emulators are needed for interfaces that do not yet exist or are not yet mature enough for test use. Test data generators to simulate various data transmissions may be required. Additional tools for test execution include: capture playback tools, drivers, interface simulators, user emulators and data generators. Network Analyzers are used to monitor and analyze the data that is transmitted over the network. Capture Playback Tools are used for replaying user sessions for regression testing, and to emulate multiple virtual sessions for system load and performance tests.

Test management tools record test results and aid in test result data analysis. These tools include loggers and other recording devices and reduction and analysis programs. File comparison utilities may be needed to compare data output with data input. A data reduction utility is needed to reduce large amounts of output data, such as output data from the PGS, to some meaningful evaluation of the data quality. The history log and systems logs gathered by CSMS system management tools and agents will be used to aid in the data analysis phase of testing.

The capture playback tool selected was XRunner, and the user emulation tool selected was LoadRunner. Both of these tools were developed by Mercury Interactive Corporation. The selection is defined in the EDS/ECS Source Evaluation Recommendation for Automated Test Tool Procurement (RFP #013). Hewlett Packard OpenView is the selected Enterprise Management Framework that will be used to monitor the network activity, loads, etc. during the testing phase. The selection is documented in the EDS/ECS Source Evaluation Recommendation for Enterprise Management Framework (July 22, 1994).

Since there is no operational data available for IR-1 testing, test data is either provided from organizations holding appropriate data (i.e., TSDIS) or must be provided by a data generator. As ECS matures in future releases, the types and formats needed to satisfy test case needs will differ. Test data needed for IR-1 is provided in Appendix A of this document.

Specific test tools and test data needed for IR-1 CSMS I&T Organization will be identified as test cases are developed and identified in Appendix A of this document.

### **3.3.4.3 Discrepancy Reporting and Resolution**

CSMS is required to report any noncompliance to Level 4 requirements encountered during CSMS I&T activities. The CSMS I&T organization will use the ECS selected COTS tool for tracking non conformance's. It is the responsibility of the CSMS I&T organization to assure that all testers are trained to use the Non conformance Reporting and Corrective Action (NRCA) system. The CSMS I&T staff will have the proper authority and access to the NRCA tool before any CSMS I&T activities begin. It is the responsibility of each tester to properly enter all

discrepancies encountered during testing into the NRCA system. Once the discrepancy is corrected, regression testing is done to make sure no new problems have been introduced by the fix. If necessary, the tester will develop additional tests to ensure the problem is satisfactorily corrected. Quality Assurance representatives are responsible for audits to ensure reported non conformance's are resolved and properly verified.

#### **3.3.4.4 Test Items Under Configuration Control**

ECS CSMS I&T organization test documents, software and hardware configurations under test, test data sets, and software and hardware tools used for testing are maintained by CM. CSMS I&T will use the ECS selected COTS tool for configuration management control. It is the responsibility of the CSMS I&T organization to train all testers to use the CM tool. The CSMS I&T staff will have the proper authority and access to unit tested components using the CM tool before any CSMS I&T activities begin. Unit-tested components entered in the CM system are accessed by the CSMS testers. These components are verified and integrated by the CSMS I&T staff. Verified segment threads and builds are entered into the CM system upon successful completion of CSMS I&T verification activities. These are made available to the System I&T test team. The responsibility to provide CM at the DAACs is a CSMS requirement. The CM tool selected for the DAACs (Clearcase) is the same tool that is used at the EDF.

If any discrepancies (see section 3.3.4.3) are found during CSMS I&T activities, CM tracks the product changes and versions that result from correcting discrepancies.

### **3.4 CSMS I&T Organizations Roles and Responsibilities**

The CSMS I&T test team roles include the following test positions and their corresponding responsibilities.

**Test Conductor** - A CSMS I&T member to conduct test execution. This person is responsible for establishing a stable and well-defined test configuration before testing takes place. This person is also responsible for collecting test outputs and recording test results. Any problems encountered during testing are entered into the NRCA System by the test conductor.

**Test Participants** - CSMS I&T members and members of the segment development organization to perform subsystem integration and support test execution. Other supporting organizations include Maintenance and Operations (M&O) and Configuration and Data Management (CM). The ECS maintenance and operations organization will support the test members in the installation and configuration of the test environment and will support the test team if any system faults are encountered during testing. This would include such instances as computer software or hardware failures which cause the test configuration to be corrupted. M&O will be responsible for reconfiguring the system as needed to continue testing. CM will provide a controlled environment for the storing and maintaining of information about the test environment including hardware, software and test tool environments. CM also stores and catalogs test documents and test input data and output data.

Test Witnesses - Individuals invited to directly observe test conduct. This will include members from the System I&T organization and the IATO as appropriate in support of System I&T and IATO testing.

Test Monitors - The Quality Assurance organization is responsible for reviewing test data, materials, and documentation. These individuals need not be present during test conduct.

### **3.5 CSMS I&T Release Testing**

CSMS I&T verification activities occur for each ECS formal release. This presently includes four Releases (A to D) and an Interim Release (IR-1). All releases follow the same formal release development track, with two exceptions for IR-1. Verification for IR-1 does not include a separate Critical Design Review and Test Readiness Review. Also, Acceptance Testing and Independent Verification and Validation (IV&V) is not performed for IR-1. For all other Releases, CSMS conducts a series of Test Readiness Reviews (TRR) and Element Test Reviews (ETR).

TRRs are informal reviews conducted incrementally as portions of the CSMS are unit tested. As software units for each Release are developed and unit tested, informal TRRs are held to determine if the software units are ready for integration and test. Test procedures are reviewed at each TRR to determine if they are complete. If the software and test procedures are deemed ready, the CSMS I&T organization integrates and tests the software.

ETRs are informal reviews conducted incrementally as portions of the CSMS are integrated and tested. Each ETR reviews the results of the portion of the CSMS just integrated and tested. The reviews ensure that components are properly integrated and that segment level requirements are met.

When all CSMS software is developed and successfully integrated and tested, and informal TRRs for a Release are completed, a formal TRR is conducted to determine test readiness of the whole CSMS segment for that Release. A final, formal ETR is held to review the results of all integration and test activities held CSMS for that Release. After the final ETR, CSMS software is delivered to System I&T for integration with other segment software.

### **3.6 CSMS I&T Schedule Overview**

#### **3.6.1 Release Schedule**

The following table (Table 3.6-1) shows CSMS I&T organizational activities across all ECS Releases. Program releases are indicated in the left most column of the chart. Program milestones are indicated across the top of the chart. For each release, CSMS I&T activities performed for each milestone are indicated. Dates for the milestones can be found in the Segment Release Plan (DID 307/DV2).

**Table 3.6-1. CSMS I&T Release Schedule**

<b>Release</b>	<b>PDR/IDR</b>	<b>CDR</b>	<b>TRR</b>	<b>ETR</b>	<b>CSR</b>
IR-1	N/A		N/A	<ul style="list-style-type: none"> <li>- conduct ETR upon completion of each segment level thread/build for IR-1</li> <li>- conduct a final ETR for entire segment for IR-1</li> </ul>	<ul style="list-style-type: none"> <li>- IR-1 CSMS I&amp;T Reports (DID 324/DV3)</li> </ul>
A	<ul style="list-style-type: none"> <li>- produce Release A CSMS I&amp;T Plan (DID 319)</li> </ul>	<ul style="list-style-type: none"> <li>- produce Release A CSMS I&amp;T Procedures (draft) (DID 322/DV3)</li> </ul>	<ul style="list-style-type: none"> <li>- conduct TRR upon completion of all unit development for Release A</li> <li>- produce Release A CSMS I&amp;T Procedures (DID 322/DV3)</li> </ul>	<ul style="list-style-type: none"> <li>- conduct ETR upon completion of each segment level thread/build Turnover to the system test organization for Release A</li> <li>- conduct a final ETR for entire segment for Release A</li> </ul>	<ul style="list-style-type: none"> <li>- Release A CSMS I&amp;T Reports (DID 324/DV3)</li> </ul>
B	<ul style="list-style-type: none"> <li>- produce Release B CSMS I&amp;T Plan (DID 319)</li> </ul>	<ul style="list-style-type: none"> <li>- produce Release B CSMS I&amp;T Procedures (draft) (DID 322/DV3)</li> </ul>	<ul style="list-style-type: none"> <li>- conduct TRR upon completion of all unit development for Release B</li> <li>- produce Release B CSMS I&amp;T Procedures (DID 322/DV3)</li> </ul>	<ul style="list-style-type: none"> <li>- conduct ETR upon completion of each segment level thread/build Turnover to the system test organization for Release B</li> <li>- conduct a final ETR for entire segment for Release B</li> </ul>	<ul style="list-style-type: none"> <li>- Release B CSMS I&amp;T Reports (DID 324/DV3)</li> </ul>
C	<ul style="list-style-type: none"> <li>- produce Release C CSMS I&amp;T Plan (DID 319)</li> </ul>	<ul style="list-style-type: none"> <li>- produce Release C CSMS I&amp;T Procedures (draft) (DID 322/DV3)</li> </ul>	<ul style="list-style-type: none"> <li>- conduct TRR upon completion of all unit development for Release C</li> <li>- produce Release C CSMS I&amp;T Procedures (DID 322/DV3)</li> </ul>	<ul style="list-style-type: none"> <li>- conduct ETR upon completion of each segment level thread/build Turnover to the system test organization for Release C</li> <li>- conduct a final ETR for entire segment for Release C</li> </ul>	<ul style="list-style-type: none"> <li>- Release C CSMS I&amp;T Reports (DID 324/DV3)</li> </ul>
D	<ul style="list-style-type: none"> <li>- produce Release D CSMS I&amp;T Plan (DID 319)</li> </ul>	<ul style="list-style-type: none"> <li>- produce Release D CSMS I&amp;T Procedures (draft) (DID 322/DV3)</li> </ul>	<ul style="list-style-type: none"> <li>- conduct TRR upon completion of all unit development for Release D</li> <li>- produce Release D CSMS I&amp;T Procedures (DID 322/DV3)</li> </ul>	<ul style="list-style-type: none"> <li>- conduct ETR upon completion of each segment level thread/build Turnover to the system test organization for Release D</li> <li>- conduct a final ETR for entire segment for Release D</li> </ul>	<ul style="list-style-type: none"> <li>- Release D CSMS I&amp;T Reports (DID 324/DV3)</li> </ul>

### **3.6.2 CSMS I&T Schedule for IR-1**

Since the specific schedule may change, please see the scheduling information located in the ECS Intermediate Logic Network (CDRL 194-108-MG2) to determine exact dates. The individual threads and builds as documented in the Build/Thread Plan (Figure 3.2-1) are also in the ECS Intermediate Logic Network with specific dates. For a general schedule of the CSMS I&T for IR-1 please see the timeline at the bottom of Figure 3.2-1 (this will show the duration planned to test each build/thread, but not the specific date the test will occur).

## 4. IR-1 Test Descriptions

---

The following sections identify all revised CSMS related Ir-1 I&T test cases. These test cases replace those found in this section in the previous version of this document. First, threads are identified. Threads are the aggregation of unit tested components (HWCIs, CSCIs, CSUs, COTs software). Each thread demonstrates a CSMS function. Builds are the integration of threads and are identified after each series of threads and/or builds which make up the build. Test cases are identified for each thread and build. The primary objective of each test case is to verify and evaluate the capabilities of each function as stated in Level 4 requirements. All of the CSMS thread and build test cases will be executed in the EDF at the Landover, Maryland facility.

### 4.1 DCE Infrastructure Thread Test

This thread demonstrates the functionality of providing authentication service for IR-1. This service includes secure user logon/logoff and maintenance of the user authentication directory. This service is provided via DCE security services.

The objective of this thread is to prove that user authentication is valid, reliable, and secure and that the user authentication directories can be maintained reliably.

Special resources required for this thread test include:

- XRunner
- HP OpenView
- Network analyzer

#### 4.1.1 Test Case 1.1: User Authentication (TC003.001)

This test case demonstrates a successful logon capability and the ability to interface with the authentication database.

##### Test Inputs

A valid ID and a valid password.

Using the command line and GUI interfaces provided by the security management application service view the authentication database.

##### Test Steps

Run an XRunner script that logs on and logs off using three valid ID/Password combinations.

Gather the information using a network analyzer, verify that the password is not readable over the network.

### Test Outputs

Screen outputs showing the success or failure of the logon/logoff attempts. Response times of each logon and logoff event. Network monitor output showing the data transmitted between the client and server.

### Success Criteria

Three successful logon and logoff attempts with each event occurring in under 15 seconds. No in the clear password data on the network.

### Assumptions and Constraints:

Until more is known about the physical design of IR-1, test cases that evaluate performance such as the response requirements depicted above cannot be adequately designed. This purpose here is to establish a place holder to evaluate what is a reasonable response time for a logon and to provide for testing the proposed configuration to provide it.

## **4.1.2 Test Case 1.2: Failed User Authentication (TC003.002)**

This test case demonstrates the ability to detect an invalid logon (UNIX and DCE).

### Test Inputs

<u>ID</u>	<u>Password</u>
Valid ID	Invalid Password
Invalid ID	Valid Password
Invalid ID	Invalid Password
Null ID	(Valid Password)
Null ID	(Invalid Password)
Valid ID	Null Password

### Test Steps

Run an XRunner script that logs on using the above combinations.

Attempt each logon 3 times. (For test purposes logon termination will be set at 3 failed attempts.)

Using a network analyzer, verify that the user logon did not pass from the security registry to the client.

### Test Outputs

Screen outputs showing the success or failure of the logon/logoff attempts. Response times of each logon and logoff event. Network monitor output showing the data transmitted between the client and server. Event log data.

### Success Criteria

All attempts at logon rejected and event log data that shows each failed logon with the appropriate data such as IDs and Passwords attempted. Logon process terminated after three

unsuccessful attempts. No error messages given that would aid in determining a valid ID password combination. The Data Encryption Standard (DES) for encryption and decryption of data is supported.

#### Assumptions and Constraints:

Logon termination set at three unsuccessful attempts. If an invalid logon occurs the error message provided will not indicate which input (ID or password) was invalid. For DCE logons when an invalid (unregistered) user id is attempted, you will not be prompt for a password.

### **4.1.3 Test Case 1.3: User Password Change (TC003.003)**

This test case demonstrates the ability of a user to change their password.

#### Test Inputs

A valid ID and a valid password.

A valid password, a new password, a repeat new password.

#### Test Steps

Run an XRunner script that:

1. Logs on.
2. Changes password.
3. Logs off.
4. Logs on with the new password.
5. Logs off.
6. Attempt logon with old password.

#### Test Outputs

Screen outputs showing the success or failure, when applicable, of the logon/logoff attempts.

#### Success Criteria

Successful logon with the changed password. Old password logon fails.

#### Assumptions and Constraints:

Since it is necessary for XRunner to enter the existing and new passwords, the passwords will be visible in the XRunner script. To minimize the risk of intrusion the password will be stored as a variable in the script that will be assigned a value just prior to the test. Test case 1 must pass.

#### **4.1.4 Test Case 1.4: User Password Reset (TC003.004)**

This test case demonstrates the ability of an administrator to reset a user password.

##### Test Inputs

A password reset for a specific ID.

The valid ID and reset password.

A reset password, a new password, a repeat new password.

The valid ID and the new password

##### Test Steps

Run an XRunner script that:

1. Resets a user password using an administration ID.
2. Does a user logon with the ID and reset password.
3. Does a password change.
4. Logs off.
5. Logs on with the new password.
6. Logs off.
7. Attempt logon with reset password.
8. Attempt logon with old password.

##### Test Outputs

Screen outputs showing the success or failure of the logon/logoff attempts.

##### Success Criteria

Successful logon with the reset password.

A forced password change.

Successful logon with the changed password.

Failed log on with reset and old password.

##### Assumptions and Constraints:

Test case 1 must pass.

#### **4.1.5 Test Case 1.5: Security Registry Maintenance (TC003.005)**

This test case demonstrates the ability of an administrator maintain the security registry.

##### Test Inputs

A valid administrator ID and password.

Valid add, change and delete registry commands.

Valid access control privileges.

##### Test Steps

Run an XRunner script that:

1. Executes a security administrator login.
2. Performs add, change and delete commands to the security registry.
3. Verify that the user accounts contain username, password, group and user identification code, login directory and command line interpreter
4. Log off.
5. Creates a security registry file report.
6. Log on with user ID.
7. Perform add, change and delete commands to the security registry.
8. Verify that the Security Management Application Service provides the capability to set, maintain and update the access control (i.e., read, write, execute privileges) information for ECS resource.
9. Log off.
10. Executes a logon to a server.
11. Perform change of password for the server.
12. Verify that the server recognizes the new password and ensure that there is a valid login prompt.
13. Log off.
14. Creates a security registry file report.
15. Verify that the Security Management Application Service provides the capability to set, maintain and update the access control (i.e., read, write, execute privileges) information for ECS resource.
16. Leave server at the login prompt.

##### Outputs

A security registry report.

### Success Criteria

Validation by the security registry report that the adds, changes, and deletes were properly made. User ID attempts to maintain directory are rejected.

### Assumptions

None.

## **4.1.6 Test Case 1.6: Security Privilege Test (TC003.006)**

This test case demonstrates system level privilege integrity.

### Test Inputs

A set of three valid IDs and passwords with different system privileges.

### Test Steps

Run an XRunner script that:

1. Logs on and logs off using three valid ID/Password combinations.
2. For each ID/Password combination use privileges allowed (file access, directory update, operator functions, etc.)
3. For each ID/Password combination use privileges not allowed (file access, directory update, operator functions, etc.)

### Test Outputs

Screen outputs showing the success or failure of the use of system privilege. System Management logs.

### Success Criteria

Valid privilege use allowed. Invalid privilege use disallowed. System log records showing invalid attempts.

### Assumptions

None.

## **4.1.7 Test Case 1.7: Server Authentication (TC003.007)**

This test case demonstrates a successful server logon capability and the ability to interface with the authentication database.

### Test Inputs

DCE cell with an account in the DCE registry.

Using the command line and GUI interfaces provided by the security management application service view the authentication database.

### Test Steps

Run an XRunner script that logs on and logs off using three valid DCE machines.

Gather the information using a network analyzer, verify that the account name is *hosts/<machine-name>/self*.

### Test Outputs

Screen outputs showing the success of the server logon attempts. Response times of each logon and logoff event.

### Success Criteria

Three successful server logon attempts with each event occurring in under 15 seconds.

### Assumptions

The three servers specified will have three separate account names. This account and its key will be created by a DCE server called **sec\_clientd**. Every 10 minutes **sec\_clientd** does the equivalent of a ktadd (using DCE security api calls). Since **sec\_clientd** runs as root, it stores the machine's keys in the default keytab file */krb5/v5srvtab*. The **sec\_clientd** daemon also performs another important function, it serves as the authenticator of the registry service.

## **4.1.8 Test Case 1.8: Authentication Expiration (TC003.008)**

This test case verifies that authentication tickets granted to users and processes expire in the configured time.

### Test Inputs

A registry data base with a test set of process and user privileges.

A set of valid user ID and passwords.

Test drivers providing process to process actions.

### Test Steps

Set ticket expiration time parameter to a short period of time.

Log users on and exercise valid user system privileges.

Run process test drivers exercising valid system privileges.

Wait till ticket expiration time expires.

Repeat user and process privilege actions.

Modify ticket expiration time and repeat the Steps.

### Test Outputs

System logs showing failed privilege attempts.

### Success Criteria

Privilege allowed prior to ticket expiration. Privilege disallowed after ticket expiration.

### Assumptions

None.

## **4.1.9 Test Case 1.9: Local Logons (rlogin) - Valid and Invalid (B01.01.01)**

This test verifies that once connection to the system (H1) is established, a tester is able to securely log on to another local host (H2), via basic LAN capabilities. All activity for each account is recorded in the history log file.

### Test Inputs

Valid account names/passwords for accounts A through F (H1), “rlogin H2” from accounts A through F, valid account names/passwords for accounts A and B (H2), invalid account names for accounts C and D (H2), valid account names but invalid passwords for accounts E and F (H2)

### Test Steps

Connection to H1 for accounts A through F.

Connection to H2 for accounts A and B.

View messages indicating incorrect logon to H2 displayed to accounts C through F.

Verify all activity is recorded in the History Log file.

### Test Outputs

Connection to H2 is established to accounts A and B, while connection to H2 is refused to accounts C through F. Messages indicating an incorrect logon is given to accounts C through F, who remain connected to H1. All activity by each account is recorded in the history log file which is verified by the tester.

### Success Criteria

The test will be deemed successfully once the connections to H2 from accounts A and B are established.

### Assumptions

None.

#### **4.1.10 Test Case 1.10: Remote Logons (Telnet H1-H2-H3) - Valid and Invalid (B01.01.02)**

This test verifies that once connection to the system (H1), or to any other local host (H2), is established, a tester is able to securely log on to a remote host (H3), via basic WAN capabilities. All activity for the account is recorded in the history log file.

##### Test Inputs

Valid account names/passwords for accounts A through F (H1), "rlogin H2" from accounts D through F, valid account names/passwords for accounts D through F (H2), "telnet H1" from accounts A through F, valid account names/passwords for accounts A and D (H3), invalid account names for accounts B and E (H1), valid account names but invalid passwords for accounts C and F (H3).

##### Test Steps

Connection to H1 for accounts A through F.

Connection to H2 for accounts D through F. Connection to H1 for accounts A and D.

View messages to accounts B, C, E, and F indicating incorrect logons and telnet sessions to H3 terminated.

Verify all activity is recorded in the History Log file.

##### Test Outputs

Connection to H3 is established to accounts A and D, while connection to H3 is refused to accounts B, C, E, and F. Messages indicating an incorrect logon is given to accounts B, C, E, and F. Accounts B and C remain connected to H1 and accounts E and F remain connected to H2.

##### Success Criteria

Connection to H3 will be established to accounts A and D; connection to H3 is refused to accounts B, C, E, and F due to incorrect logon.

##### Assumptions

None.

#### **4.1.11 Test Case 1.11: Remote Logons (Telnet H1-H3-H1) - Valid and Invalid (B01.01.03)**

This test verifies that once a connection to a remote host (H3) from the local host (H1), a tester is able to securely log back into the local host (H1), via basic WAN capabilities. This test verifies that connection into the LAN from the WAN is possible.

##### Test Input

Valid account names/passwords for accounts A through F (H1), "telnet H3" from accounts A through F, valid account names/passwords for H3. "telnet H1" from accounts A through F from

H3, valid account names/passwords for accounts A and D (H1), invalid account names for accounts B and E (H1), valid account names but invalid passwords for accounts C and F (H1).

#### Test Steps

Connection from H1 for accounts A through F.

Connection to H3 for accounts A through F.

Connection to H1 for accounts A and D.

View messages to accounts B, C, E, and F indicating incorrect logons and telnet sessions to H1 terminated.

Verify all activity is recorded in the History Log file.

#### Test Outputs

Connection to H1 is established for accounts A and D, while connection to H1 is refused for accounts B, C, E, and F.

#### Success Criteria

Connection to H1 will be successful for accounts A and D and accounts B, C, E, and F will be refused.

#### Assumptions

None.

### **4.1.12 Test Case 1.12: Syntax and Commands Simplification (TC011.001)**

The purpose of Syntax and Commands Simplification is to verify that the complex DCE syntax and commands have been incorporated into easy-to-use objects.

#### Test Inputs

Inputs to this test case include use of the OODCE class libraries.

#### Test Steps

Verify that the OODCE class libraries exist

Call the libraries

Verify that the available objects are easy to use

#### Test Outputs

The expected results of this test include successful use of the OODCE class libraries

#### Success Criteria

This test will be deemed successful when all of the OODCE class libraries have been accessed and the objects have been executed.

#### Assumptions

None.

#### **4.1.13 Test Case 1.13: Sample Object Implementation (TC011.002)**

This test case demonstrates, using a client/server architecture, the ability to demonstrate an object created using OODCE code and then link the object to C++ bindings.

##### Test Inputs

Inputs to this test case include **TBD**.

##### Test Steps

Demonstrate an object that was created using OODCE class libraries.

Verify that the object can bind using C++.

##### Test Outputs

The expected results of this test include being able to pass objects using OODCE.

##### Success Criteria

This test will be deemed successful when all objects developed using OODCE can bind to the client/server architecture.

##### Assumptions

None

#### **4.1.14 Test Case 1.14: Logoffs - Normal (B01.02.01)**

This test verifies that when a tester, using a valid account, logs off a system or a host, the connection is properly closed to the system or the host.

##### Test Inputs

Valid account names/passwords for accounts A and B on Hosts 1, 2, and 3, “rlogin Host 2”, “telnet Host 3”, logoff.

##### Test Steps

Account A connects to the system on Host 1, logs on to a local host (Host 2), then logs on to a remote host (Host 3).

Log off the remote host (Host 3), then the local host (Host 2), and finally Host 1.

In each instance, another tester, using another valid account, is monitoring the system on each host to verify that connection to the host has been closed for account A.

Verify that all logon and logoff activity is recorded in the history log file.

##### Test Outputs

Account B monitors the activity of account A, history log file records that have corresponding logon and logoff records.

### Success Criteria

Account B verifies that connection is established for account A on the different hosts when account A logs on and that connection is closed when account A is logged off each host. History log files should have corresponding logon and logoff records.

### Assumptions

None.

## **4.1.15 Test Case 1.15: Logoffs - Abnormal (B01.02.02)**

This test verifies that when an abnormal event occurs and disconnects an account from the system (i.e., the tester's workstation is turned off, one of the hosts is powered off, a UNIX "kill", etc.), the system properly closes connection to the account. History log file entries are recorded for all activity. This test is to be repeated for the different types of abnormal events that will cause a disconnect from the system.

### Test Inputs

Valid account names/passwords for accounts A and B on Hosts 1, 2, and 3, "rlogin Host 2", "", an abnormal termination of account A to the system.

### Test Steps

For accounts A and B, perform proper log onto Host 1.

rlogin Host 2.

telnet Host 3.

Turn off workstation for account A.

Verify history log file records.

Repeat for a powered off host.

Repeat for a UNIX kill command.

### Test Outputs

Account B monitors activity of account A, history log file records which include a record that indicates that account A was logged out of Host X due to a system error. Port connection the host is properly closed.

### Success Criteria

History log file records which include a record that indicates that account A was logged out of Host X due to a system error. The port connection to the host is closed. If one of the hosts was powered off, then the tester waits to log back on once the host is powered back on.

### Assumptions

None.

#### **4.1.16 Test Case 1.16: Login to EDF (T01-02.02.01)**

This test verifies that the tester is able to successfully logon to a host machine within the EDF.

### Test Inputs

Valid account name/password for tester on host within EDF.

### Test Steps

Perform standard login on EDF host machine.

Verify history log file.

### Test Outputs

Successful logon. History log file updated with tester activities.

### Success Criteria

Connection to the system is established and the main screen of the host is displayed to the tester. The history log file is updated with the tester's logon activities.

### Assumptions

None.

## **4.2 Messaging and File Transfer Thread Test**

This thread demonstrates the messaging and file transfer functionality of IR-1. This tread will demonstrate the ECS message transfer capability across the internet, via E-Mail services, to designated user workstations. Other internet utilities will also be verified, as will the ftp file transfer methodology, as it applies to Ir-1.

Special resources required for this thread test include:

- XRunner
- HP OpenView
- Network analyzer

#### **4.2.1 Test Case 2.1: Internet Utilities Test (TS002.014)**

### Description

This test verifies the capability to browse WWW, to read from and post USENET newsgroups, read and send electronic mail via the Internet and provide access to a gopher and WAIS clients.

### Test Inputs

Inputs to this test include URL locations and email messages.

### Test Steps

TBD

### Test Outputs

Outputs to this test include Email messages and URL locations.

### Success Criteria

This test is successful if the ability to receive and distribute news, email, and WWW URLs over the Internet is demonstrated.

### Assumptions

None.

## **4.2.2 Test Case 2.2: Bulletin Board (BC012.004)**

The purpose of the Bulletin Board test is to demonstrate the capability of interactive functionality for any bulletin board users. The bulletin board will be tested for the capability of users to either subscribe or unsubscribe to any bulletin board and to select a subscribed bulletin board for viewing all messages in that bulletin board. Capability of the bulletin board to respond to a message by sending the response to the bulletin board and/or to the author and/or any other user specified destination, will be tested.

The following search capability will be tested for bulletin board users:

- a. search for a string in message headers and in message text
- b. search by author
- c. search by subject

A catch-up feature which excludes user specified messages from appearing in the bulletin board when it is viewed next time, will be tested. The bulletin board services must demonstrate that users can post messages to bulletin board(s), maintain an access history for each bulletin board per user basis, which tracks the messages read by the user for each bulletin board. Saving messages to the local bulletin board system will be tested, along with attaching ASCII or binary files to a message being sent. Also, a means to retrieve files will be tested.

The BBS must demonstrate the following bulletin board configuration options:

- a. screen size
- b. number of messages displayed on a screen
- c. screen colors (background/foreground)
- d. read message indicator

### Test Inputs

Sequence of interactive commands simulating BBS usage for search, configuration, message retrieval, etc.

### Test Steps

Verify that the BBS is based on TCP/IP, NNTP, SMTP and USenet message standard.

Demonstrate the functionality of the BBS to support multiple bulletin boards.

Verify that multiple users (registered and non-registered) can be accessed concurrently.

Verify that each bulletin board can contain multiple messages.

Verify, as an M&O user, the ability to: create the new bulletin board, delete existing bulletin boards, delete messages from a bulletin board, back up bulletin boards, force users off a bulletin board or the entire bulletin board service for backup, collect history and or statistical information and back up bulletin boards.

Send a message to bulletin boards.

Copy or save a posted message to their local system.

Verify the ability to respond to a posted message by sending the response message to: the bulletin board, author of the original message and named destinations.

Demonstrate the use of the Bulletin Board via interactive mode from the command line.

Demonstrate the ability of the CSS Bulletin Board Service to allow users to subscribe and/or unsubscribe to a bulletin board.

Demonstrate the capability to subscribe to a bulletin board and view a summary for each message in it.

User will respond to a message by sending the response to the bulletin board, author of the message and/or any other operator specified destination.

Using the search capability provided by the BBS: search for a string, search by author or search by subject.

Verify that a catch-up feature which excludes user specified messages from appearing in the bulletin board next time it is viewed.

### Test Outputs

Outputs include: access of multiple bulletin boards with multiple messages posted to each, new bulletin board, deleted bulletin boards, back ups, access history and statistical information, responses to messages, subscribed to bulletin boards, unsubscribed bulletin boards, and copy or saves of a message to their local system.

### Success Criteria

When all validation and verification of all BBS functions have been determined to have satisfied the overall test requirements.

### Assumptions

None.

### **4.2.3 Test Case 2.3: E-Mail (TC006.002)**

The E-Mail test will demonstrate the capability of the messaging service to manage and interact with user E-mail. This mailbox will be tested for, copying and/or moving messages from the MAILBOX to the user defined folders, and for providing an access control feature which requires authentication for access to the Mailtool via login and password. The MAILBOX will also be tested for allowing users to set an automatic time period for deletion of messages to help manage the MAILBOX size, by removing old messages after confirmation. The message editor will be tested for the capability of composing messages, by providing a title/subject field for the message and various destinations.

### Test Inputs

Inputs require creating a user defined MAILBOX which will store incoming messages in the mailbox folders, created for long term archiving. Summary status for all mail messages will be verified. A reply to a message. A composed message over the editor. Sending a message, creating a private mailing list and creating a public mailing list.

### Test Steps

Demonstrate the capability to access the electronic mail service in interactive mode.

Reply, to the author and to all destinations addressed in the incoming message.

Verify that a "MAILBOX" is provided, where the incoming messages are stored.

Demonstrate the availability of operator defined folders for archiving and verify that you can copy/move messages from the "MAILBOX" to specified folders.

Retrieve a summary of all messages, containing at a minimum title/subject and name of author.

Verify that an editor is provided to compose a message and that there is a provided title/subject field for a message.

Send the message to multiple destinations (repeat for: a single user, an operator manned position, a mailing list, and a site which consists of several operators).

Create a private mailing list, verify that the lists can contain multiple destinations for individual operators.

Create a public mailing list, verify that the list contains multiple destinations accessible to all operators.

### Test Outputs

The expected results of these tests are a successful demonstration of all the required interactive user functions provided by the MAILBOX and folder. Validation and verification of each test must be complete and satisfactory. A reply to a message, an archived message, summary of all messages, private and public mailing lists.

### Success Criteria

When all validation and verification of all Mailtool functions have been determined to have satisfied the overall test requirements.

### Assumptions

None.

## **4.2.4 Test Case 2.4: EDF to DAAC Message Transfer (TC010.001)**

The EDF to DAAC message transfer test will demonstrate E-mail message transfer capability, TO and FROM the EDF workstation. This test will include, *single* message transfers TO and FROM a single DAAC, and a *distributed* message transfer FROM EDF TO all DAACs.

### Test Inputs

Inputs include, creating a simple mail message to transfer across the internet from the EDF workstation and receiving a mail message from the internet DAACs on the EDF workstation.

### Test Steps

#### *Single message transfer*

- Login on EDF workstation
- Mail message to each DAAC individually
- Check for successful transfer confirmation

#### *Distributed message transfer*

- Login on EDF workstation
- Mail message to each DAAC simultaneously
- Check for successful transfer confirmation

Receive message transfer from remote DAAC workstation

- Transfer mail message from a remote DAAC workstation to EDF workstation
- Login on EDF workstation
- Enter: mail
- Verify new message received in mailbox

### Test Outputs

The expected results of this test include successful message transfers TO and FROM the designated IR1 workstations, as they're defined in each test.

### Success Criteria

When a validation and verification of all messages transferred or received have been determined successful TO and FROM the designated workstations.

### Assumptions

All workstations are configured to transfer and receive mail messages via E-mail.

## **4.2.5 Test Case 2.5: E-Mail from EDF to GSFC (T01-02.05.01)**

This test verifies that a tester using valid accounts, via basic LAN and WAN capabilities, is able to send e-mail messages from an account at EDF to an account at GSFC.

### Test Inputs

Valid account names/passwords for accounts at both EDF and GSFC. Tester sends e-mail message from EDF account at GSFC.

### Test Steps

Connection to the respective hosts, message received by account at GSFC.

### Test Outputs

Tester receives e-mail message from EDF at GSFC. History log file will record all activities and transactions.

### Success Criteria

The email from EDF to GSFC is transmitted successfully.

### Assumptions

None.

## **4.2.6 Test Case 2.6: E-Mail from EDF to LaRC (T01-02.05.02)**

This test verifies that a tester using valid accounts, via basic LAN and WAN capabilities, is able to send e-mail messages from an account at EDF to an account at LaRC.

### Test Inputs

Valid account names/passwords for accounts at both EDF and LaRC. Tester sends e-mail message from EDF account at LaRC.

### Test Steps

Connection to the respective hosts, message received by account at LaRC.

### Test Outputs

Tester receives e-mail message from EDF at LaRC. History log file will record all activities and transactions.

### Success Criteria

The email transmission from EDF to LaRC completes successfully.

### Assumptions

None.

## **4.2.7 Test Case 2.7: SCF to DAAC Message Transfer (TC010.002)**

The SCF to DAAC message transfer test will demonstrate E-mail message transfer capability, TO and FROM the SCF workstation. This test will include, *single* message transfers TO and FROM a single DAAC, and a *distributed* message transfer FROM SCF TO all DAACs (may be emulated).

### Test Inputs

Inputs include, creating a simple mail message to transfer across the internet from the SCF workstation and receiving a mail message from the internet DAACs on the SCF workstation.

### Test Steps

#### *Single message transfer*

- Login on SCF workstation
- Mail message to each DAAC individually
- Check for successful transfer confirmation

#### *Distributed message transfer*

- Login on SCF workstation
- Mail message to each DAAC simultaneously
- Check for successful transfer confirmation

#### *Receive message transfer from remote DAAC workstation*

- Transfer mail message from a remote DAAC workstation to SCF workstation
- Login on SCF workstation
- Enter: mail
- Verify new message received in mailbox

### Test Outputs

The expected results of this test include successful message transfers TO and FROM the designated IR1 workstations, as they're defined in each test.

### Success Criteria

When a validation and verification of all messages transferred or received have been determined successful TO and FROM the designated workstations.

### Assumptions

All workstations are configured to transfer and receive mail messages via E-mail. If available for use may use real SCF. If an SCF is not available we will emulate the functionality.

## **4.2.8 Test Case 2.8: E-Mail from EDF to EDC (T01-02.05.04)**

This test verifies that a tester using valid accounts, via basic LAN and WAN capabilities, is able to send e-mail messages from an account at EDF to an account at EDC.

### Test Input

Valid account names/passwords for accounts at both EDF and EDC. Tester sends e-mail message from EDF account at EDC.

### Test Steps

Connection to the respective hosts, message received by account at EDC.

### Test Outputs

Tester receives e-mail message from EDF at EDC. History log file will record all activities and transactions.

### Success Criteria

The e-mail message from EDF to EDC completes successfully.

### Assumptions

None.

## **4.2.9 Test Case 2.9: DAAC to DAAC Message Transfer (TC010.003)**

The DAAC to DAAC message transfer test will demonstrate E-mail message transfer capability, TO and FROM the DAAC workstations. This test will include, *single* message transfers TO and FROM a single DAAC, and a *distributed* message transfer TO and FROM all DAACs.

### Test Inputs

Inputs include, creating a simple mail message to transfer across the internet from one DAAC workstation and receiving a mail message from the internet DAACs on the same DAAC workstation.

### Test Steps

#### *Single message transfer*

- Login on DAAC workstation
- Mail message to each DAAC individually
- Check for successful transfer confirmation

#### *Distributed message transfer*

- Login on DAAC workstation
- Mail message to each DAAC simultaneously
- Check for successful transfer confirmation

#### *Receive message transfer from remote DAAC workstation*

- Transfer mail message from a remote DAAC workstation to DAAC workstation
- Login on DAAC workstation
- Enter: mail
- Verify new message received in mailbox

### Test Outputs

Successful message transfer confirmation and the verification

### Success Criteria

All message transfer completes successfully.

### Assumptions

None.

## **4.2.10 Test Case 2.10: E-Mail from DAAC to DAAC (T01-02.05.05)**

This test verifies that a tester, using valid accounts, is able to send e-mail between DAAC sites. This test will be completed at each DAAC site.

### Test Input

Valid account names/passwords for accounts at both DAACs. Tester sends e-mail message from site to site.

### Test Steps

Connection to the respective hosts, message received by account at DAAC 2.

### Test Outputs

Tester receives e-mail message from DAAC 1 at DAAC 2. History log file will record all activities and transactions.

### Success Criteria

The account at DAAC 2 connects successfully.

### Assumptions

None.

## **4.2.11 Test Case 2.11: E-Mail- Asynchronous Messaging (TC006.001)**

The purpose of the E-mail test case is to demonstrate the availability of asynchronous messaging (loosely coupled with a single message queue) and to verify the protocols in which the external mail system is based.

### Test Inputs

Inputs to this test case include a variety of asynchronous messages.

### Test Steps

Using XRunner create a script to conduct the following activities:

- Create an E-mail message (with valid address).

- Send the message.

- Inspect the protocol to verify that the electronic mail service interoperates and exchanges messages with external mail systems based on the SMTP protocol.

- Verify receipt of the message and that the content is correct.

- Create an E-mail message (with an invalid address).

- Send the message.

- Verify notification of non delivery.

- Repeat for X.400 protocol.

### Test Outputs

Outputs include receipt of valid E-mail message and notification of message not delivered. Mail message sent via the SMTP and X.400 protocols.

### Success Criteria

This test will be deemed successful when all of the above procedures have been executed.

### Assumptions

None.

#### **4.2.12 Test Case 2.12: Sending E-Mail Messages to Local and Remote Hosts (B01.05.01)**

This test verifies that a tester using a valid account, via basic LAN and WAN capabilities, is able to e-mail messages to other accounts on the same host (H1), on a local host (H2), or on a remote (H1) host. In all cases, records of the transactions are recorded in the history log file.

##### Test Input

Valid account names/passwords for account A on local H1, account B on local H1, account C on local H2, and account D on remote H1. Message 1 sent from account A to account B. Message 2 sent from account A to account C. Message 3 sent from account A to account D.

##### Test Steps

Connection to the respective hosts, message 1 received by account B, message 2 received by account C, and message 3 received by account D.

History log file records of all activity and transactions by the tester.

##### Test Outputs

The history log will record the logon to the system by each account, it will record the transmission of the e-mail messages, it will record the resource usage, response time, and the number of transactions.

##### Success Criteria

The connection between accounts will successfully connect.

##### Assumptions

None.

#### **4.2.13 Test Case 2.13: Receiving E-Mail Messages to Local and Remote Hosts (B01.05.02)**

This test verifies that a tester using a valid account, via basic LAN and WAN capabilities, is able to receive e-mail messages from the same host (H1), a local host (H2), or a remote host (H1). Each message, in this case, will be sent simultaneously to the same account (account A). In all cases, records of the transactions are recorded in the history log file.

##### Test Input

Valid account names/passwords for account A on local H1, account B on local H1, account C on local H2, and account D on remote H1. Messages from accounts B, C, and D to account A.

##### Test Steps

Connection to the respective hosts, messages received by account A.

History log file records of all activity and transactions by the tester.

### Test Outputs

The history log will record the logon to the system by eachount, it will record the transmission of the e-mail messages, it will record the resource usage, response time, and the number of transactions.

### Success Criteria

The connection to the respective hosts will be successful.

### Assumptions

None.

## **4.2.14 Test Case 2.14: Client/User File Transfer (TC009.001)**

The purpose of the Client/User File Transfer test is to demonstrate communications among the appropriate DAAC workstations that are available for IR1. Demonstrate the ability of a valid IR1 user to ftp (put and get) a file to a workstation that is not in the IR1 Cell. Verify that a valid IR1 user can transfer files using the interactive transfer mode. Demonstrate the functionality of ftp commands (mput, mget, open, close, cd, ascii, binary, chmod, delete, dir, hash, image, prompt, system, type, etc. )

### Test Inputs

Inputs to this test case include a series of file transfers using ftp for various data files. The data files will be consistent, in size and content, with actual IR1 data files.

### Test Steps

Verify that there are test accounts setup on all of the IR1 implemented DAAC workstations (EDF - edf-bb, epsrver, GSFC - ecsgsfc1, ecs-global, MSFC - hydra, meteor, LaRC - ecs, nephos and EDC - ecs-hp1, ecs-alpha1).

Demonstrate that each of the workstations can transfer files to other workstations and receive files that have been transferred from other workstations.

Verify that the transfers were completed in a timely and efficient manner. Efficiency is determined not only by speed but also by the accuracy in which a file reaches its destination.

Demonstrate functionality of ftp commands.

### Test Outputs

The expected results of this test include successful file transfers (put and get) from each of the IR1 workstations. Screen outputs of expected results for each ftp command.

### Success Criteria

This test will be deemed successful when all files are transferred from their designated source to their designated destination and are verified to match the expected file. All ftp commands function as expected.

### Assumptions

None.

#### **4.2.15 Test Case 2.15: Transmit File from EDF to GSFC (ftp) (T01-02.04.01)**

This test verifies that a tester, using a valid account, is able to transmit a file from EDF to an account on host machine at GSFC. This test verifies the connectivity of the EDF LAN to the system WAN.

### Test Inputs

Valid login for tester on H1 at EDF and H2 at GSFC. Data file for file transfer (ftp) from H1 to H2.

### Test Steps

ftp completes data file transfer from H1 to H2.

H2 directory listings verify that data file was transferred.

### Test Outputs

The history log file will record the logon to both hosts, it will record the transmission of the ftp transaction, it will record the resource usage, response time, and the number of transactions. Checksum of data files on H1 and H2 should equal.

### Success Criteria

H1 and H2 will successfully transfer a data file.

### Assumptions

None.

#### **4.2.16 Test Case 2.16: Transmit File from EDF to LaRC (ftp) (T01-02.04.02)**

This test verifies that a tester, using a valid account, is able to transmit a file from EDF to an account on host machine at LaRC. This test verifies the connectivity of the EDF LAN to the system WAN.

### Test Inputs

Valid login for tester on H1 at EDF and H2 at LaRC. Data file for file transfer (ftp) from H1 to H2.

### Test Steps

ftp completes data file transfer from H1 to H2.

H2 directory listings verify that data file was transferred.

### Test Outputs

The history log file will record the logon to both hosts, it will record the transmission of the ftp transaction, it will record the resource usage, response time, and the number of transactions. Checksum of data file on H1 and H2 should equal.

### Success Criteria

The data file will successfully transmit between H1 and H2.

### Assumptions

None.

## **4.2.17 Test Case 2.17: Transmit File from EDF to MSFC (ftp) (T01-02.04.03)**

This test verifies that a tester, using a valid account, is able to transmit a file from EDF to an account on host machine at MSFC. This test verifies the connectivity of the EDF LAN to the system WAN.

### Test Inputs

Valid login for tester on H1 at EDF and H2 at MSFC. Data file for file transfer (ftp) from H1 to H2.

### Test Steps

ftp completes data file transfer from H1 to H2.

H2 directory listings verify that data file was transferred.

### Test Outputs

The history log file will record the logon to both hosts, it will record the transmission of the ftp transaction, it will record the resource usage, response time, and the number of transactions. Checksum of data file on H1 and H2 should equal.

### Success Criteria

The ftp data file transfer will complete between H1 and H2.

### Assumptions

None.

## **4.2.18 Test Case 2.18: Transmit File from EDF to EDC (ftp) (T01-02.04.04)**

This test verifies that a tester, using a valid account, is able to transmit a file from EDF to an account on host machine at EDC. This test verifies the connectivity of the EDF LAN to the system WAN.

### Test Inputs

Valid login for tester on H1 at EDF and H2 at EDC. Data file for file transfer (ftp) from H1 to H2.

### Test Steps

ftp completes data file transfer from H1 to H2.

H2 directory listings verify that data file was transferred.

### Test Outputs

The history log file will record the logon to both hosts, it will record the transmission of the ftp transaction, it will record the resource usage, response time, and the number of transactions. Checksum of data file on H1 and H2 should equal.

### Success Criteria

The data transmission from H1 to H2 completes successfully.

### Assumption

None.

## **4.2.19 Test Case 2.19: Transmit File from EDF to GSFC (rcp) (T01-02.04.05)**

This test verifies that a tester, using a valid account, is able to transmit a data file to an account on a machine at GSFC via remote file copy (rcp).

### Test Inputs

Valid login for tester on H1 at EDF and H2 at GSFC. Data file for remote file copy (rcp) from H1 to H2.

### Test Steps

rcp completes data file transfer from H1 to H2.

H2 directory listings verify that data file was transferred.

### Test Outputs

The history log file record the logon onto both hosts, it will record the transmission of the rcp transaction, it will record the resource usage, response time, and the number of transactions. Checksum of data files on H1 and H2 should equal.

### Success Criteria

The rcp completes successfully between H1 and H2.

### Assumptions

None.

#### **4.2.20 Test Case 2.20: Transmit File from EDF to LaRC (rcp) (T01-02.04.06)**

This test verifies that a tester, using a valid account, is able to transmit a data file to an account on a machine at LaRC via remote file copy (rcp).

##### Test Inputs

Valid login for tester on H1 at EDF and H2 at LaRC. Data file for remote file copy (rcp) from H1 to H2.

##### Test Steps

rcp completes data file transfer from H1 to H2.

H2 directory listings verify that data file was transferred.

##### Test Outputs

The history log file record the logon onto both hosts, it will record the transmission of the rcp transaction, it will record the resource usage, response time, and the number of transactions. Checksum of data files on H1 and H2 should equal.

##### Success Criteria

The rcp completes successfully between H1 and H2.

##### Assumptions

None.

#### **4.2.21 Test Case 2.21: Transmit File from EDF to MSFC (rcp) (T01-02.04.07)**

This test verifies that a tester, using a valid account, is able to transmit a data file to an account on a machine at MSFC via remote file copy (rcp).

##### Test Inputs

Valid login for tester on H1 at EDF and H2 at MSFC. Data file for remote file copy (rcp) from H1 to H2.

##### Test Steps

rcp completes data file transfer from H1 to H2.

H2 directory listings verify that data file was transferred.

##### Test Outputs

The history log file record the logon onto both hosts, it will record the transmission of the rcp transaction, it will record the resource usage, response time, and the number of transactions. Checksum of data files on H1 and H2 should equal.

##### Success Criteria

The rcp completes successfully between H1 and H2.

#### Assumptions

None.

#### **4.2.22 Test Case 2.22: Transmit File from EDF to EDC (rcp) (T01-02.04.08)**

This test verifies that a tester, using a valid account, is able to transmit a data file to an account on a machine at EDC via remote file copy (rcp).

#### Test Inputs

Valid login for tester on H1 at EDF and H2 at EDC. Data file for remote file copy (rcp) from H1 to H2.

#### Test Steps

rcp completes data file transfer from H1 to H2.

H2 directory listings verify that data file was transferred.

#### Test Outputs

The history log file record the logon onto both hosts, it will record the transmission of the rcp transaction, it will record the resource usage, response time, and the number of transactions. Checksum of data files on H1 and H2 should equal.

#### Success Criteria

The rcp completes successfully between H1 and H2.

#### Assumptions

None.

#### **4.2.23 Test Case 2.23: Anonymous ftp (TC009.003)**

The purpose of the Anonymous ftp test is to demonstrate the capability of non IR1 users transferring or retrieving data from the DAAC workstations. There is a special directory (/users/ftp/pub ) setup for this functionality to ensure that the DAAC workstations can not be violated by providing outside users access to the system. Verify that non IR1 users can retrieve or transfer files to this designated directory. Verify that IR1 users can post files to the directory to be retrieved from non IR1 users or retrieve the files that the non IR1 users have posted.

#### Test Inputs

Inputs to the test case include a series of file transfers (put and get) using anonymous ftp for various file sizes.

#### Test Steps

Inspect each of the DAAC IR1 workstations to ensure that it has a /users/ftp/pub directory with read/write privileges for the world.

Verify that the user is unable to access any other directories within the cell.

Place a file in this directory and verify that a non ECS user can retrieve the file by using anonymous ftp.

Verify that a non ECS user can copy a file to the same directory using anonymous ftp.

Demonstrate that a valid IR1 user can then retrieve the file that was previously transferred to the /users/ftp/pub directory.

#### Test Outputs

The expected results of this test include a report indicating that the file was successfully transferred or retrieved using anonymous ftp.

#### Success Criteria

This test will be deemed successful when non ECS users are able to retrieve files from or transfer files to the /users/ftp/pub directory on a DAAC workstation. The files that have been transferred to this directory from non ECS users will be moved to the appropriate locations by valid IR1 users.

#### Assumptions

None.

### **4.2.24 Test Case 2.24: Application File Transfer (TC009.004)**

The purpose of the Application File Transfer test is to demonstrate the ability of the application to transfer data files using API calls.

#### Test Inputs

Inputs to this test case include a series of file transfers using API calls for various data files, by calling an Ir1 application.

#### Test Steps

Verify that there are test accounts setup on all of the Ir1 implemented DAAC workstations (EDF - edf-bb, epserver, GSFC - ecsgsfc1, ecs-global, MSFC - hydra, meteor, LaRC - ecs, nephos).

Using edf-bb as the server, create a data file to initialize the transfers of various file sizes to each of the IR1 workstations (client).

This transfer of a data file will be launched throughout the day. Both receives and puts will be executed.

Analyze the data.

### Test Outputs

The expected results of this test include successful file transfers from each of the Ir1 workstations. Reports will show where deviations occur.

### Success Criteria

This test will be deemed successful when all files are transferred from their designated source to their designated destination, and are verified to match the expected file.

### Assumptions

None.

## **4.2.25 Test Case 2.25: Network Filtering Test (BC002.003)**

This test demonstrates the internetworking filtering of packets on port/socket and source and/or destination address.

### Test Inputs

Router configurations establishing filtering conditions. Test packets with combinations of port/socket identification and source/destination addresses.

### Test Steps

Run telnet, remote log on.

File transfer, and interprocess jobs that create the above described test packets.

### Test Outputs

Network management logs showing the success or failure to the various packets in getting through the internetworking filters.

### Success Criteria

Not allowed packets fail, allowed packets passed (i.e., proper address filtering). Log records of failed packets.

### Assumptions

This functionality will be further verified in other build/thread tests since internetworking will implicitly be a part of most other tests.

## **4.2.26 Test Case 2.26: Multiple Accounts Transmitting Large Data Files to GSFC DAAC (B01.07.01)**

This test verifies that multiple accounts are able to transmit large data files over the WAN to GSFC.

#### Test Inputs

Accounts A through F are logged on with valid account names/passwords. Accounts A through F will simultaneously transmit a large data file to GSFC, using ftp the "hash" option, to valid accounts at GSFC.

#### Test Steps

Accounts A through F will view their perspective screens and notice a slight delay in the rate the hashing appears.

#### Test Outputs

The history log will record each input that was initiated by each account. The system response will slow down due to the network traffic from the multiple ftp transactions.

#### Success Criteria

The multiple ftp transactions will complete successfully and the system slow down due to the network traffic.

#### Assumptions

None.

### **4.2.27 Test Case 2.27: Multiple Accounts Transmitting Large Data Files Within the EDF (B01.07.02)**

This test verifies that multiple accounts can transmit large data files over the Ethernet LAN within the EDF.

#### Test Inputs

Accounts A through G are logged on with valid account names/passwords. Accounts A through F will simultaneously transmit a large data file within the EDF to account G using ftp with the "hash" option.

#### Test Steps

Accounts A through F will view their perspective screens and notice a slight delay in the rate the hashing appears.

#### Test Outputs

The history log will record each input that was initiated by each account. The system response will slow down due to the network traffic from the multiple ftp transactions.

#### Success Criteria

The system response will slow down due to the network traffic from the multiple ftp transactions.

### Assumptions

None.

### **4.2.28 Test Case 2.28: External Interfaces Integration Test (BC002.001)**

This test case Integration tests the External interfaces implemented in Ir-1, using the Gateway concept (refer to Figures 4.2-1 and 4.2-2).

### Test Inputs

External interface test data.

### Test Steps

Run XRunner scripts that communicate test data using the appropriate real and simulated external interfaces illustrated in Figures 4.2-1 and 4.2-2.

### Test Outputs

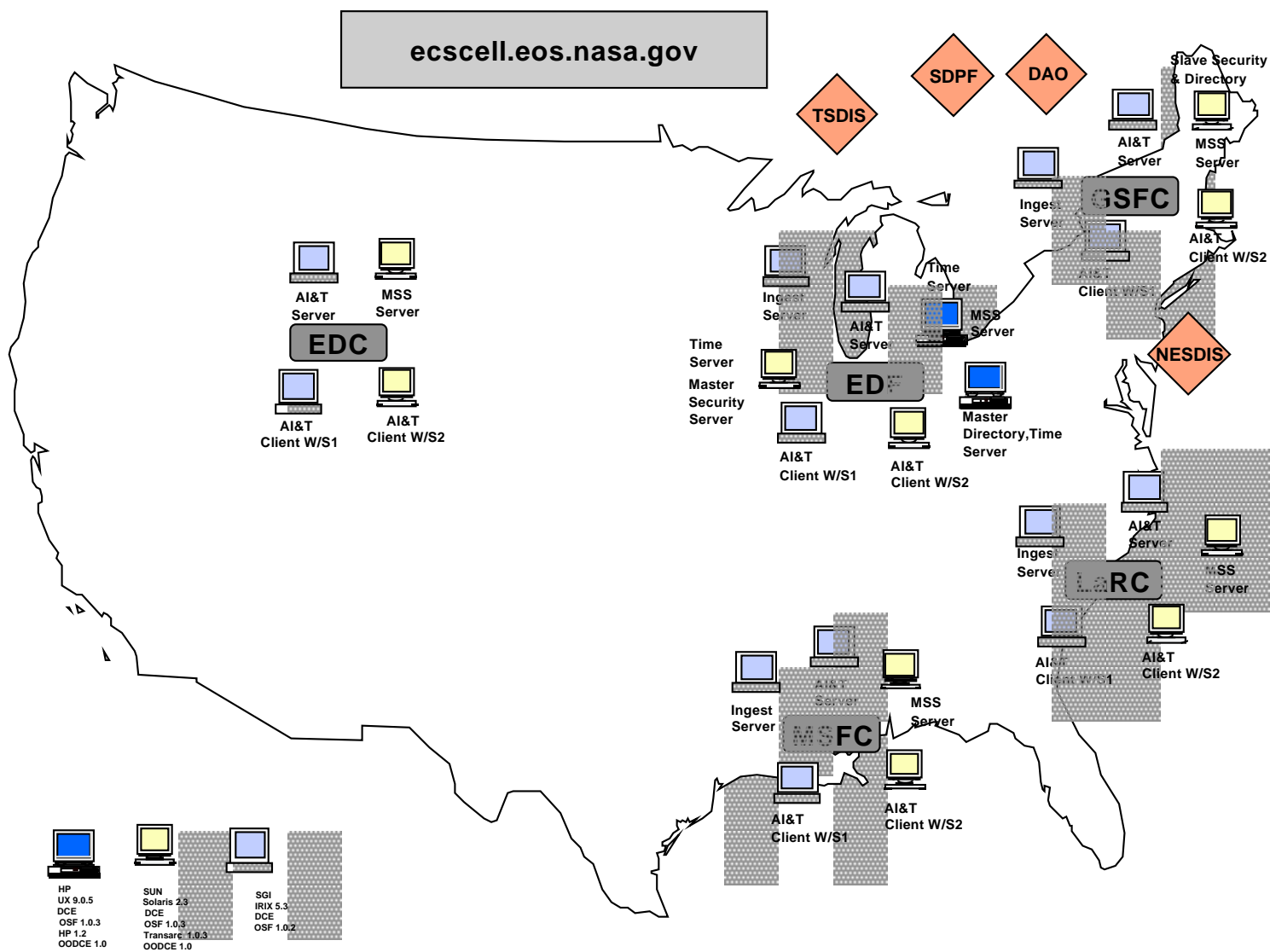
Comparisons of input and output data, System Management logs, Network analyzer outputs.

### Success Criteria

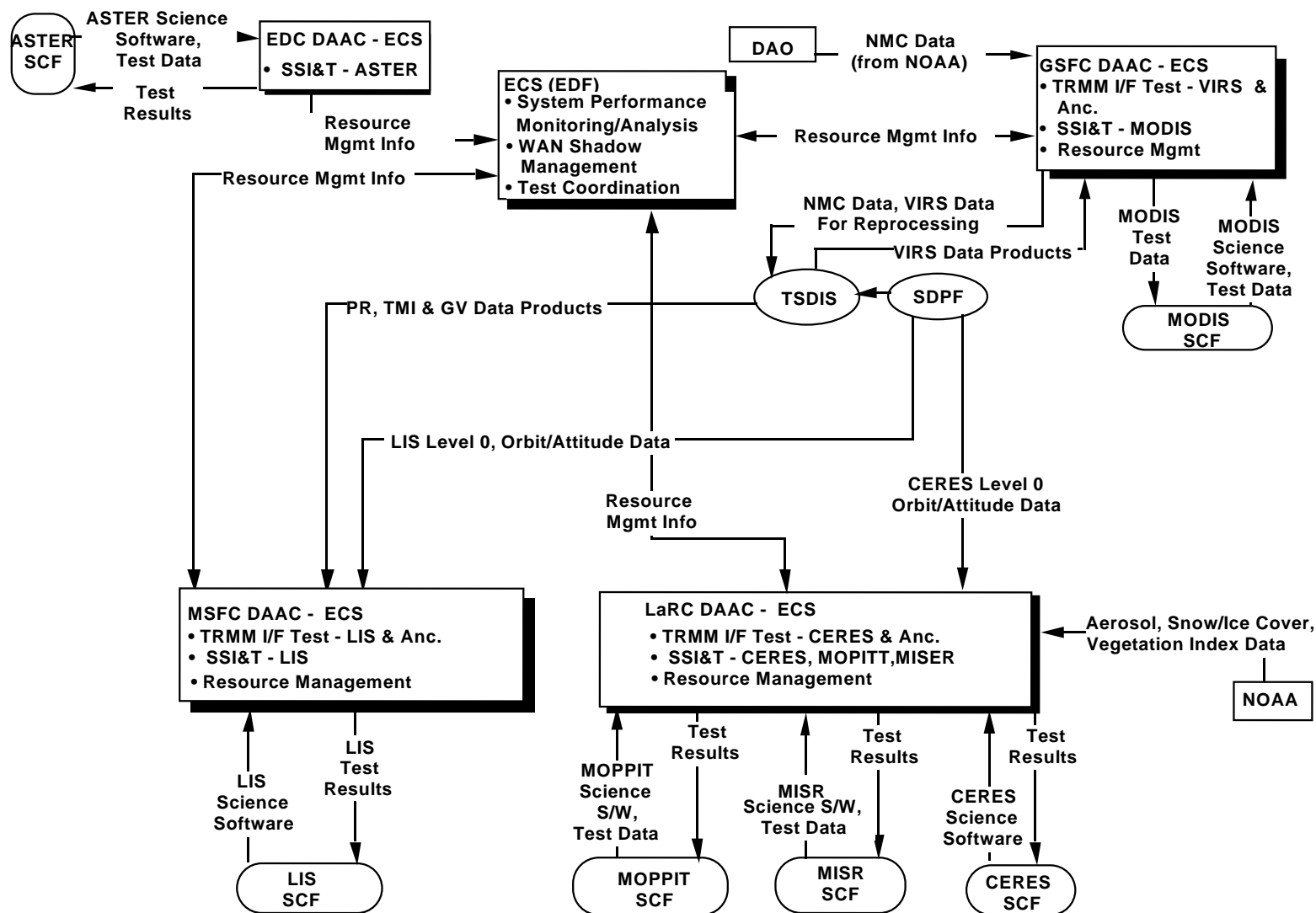
The interfaces function properly, data is communicated reliably and accurately, data volumes are reasonably for proposed network sizing.

### Assumptions and Constraints

The most current version of the Ir-1 External Interfaces diagram will be used for final test procedure preparation. Refer to the Ir-1 Mission Statement (Doc. No. 222-WP-001-001).



**Figure 4.2-1. Interim Release One DCE Cell Topology**



**Figure 4.2-2. Interim Release One External Interfaces**

#### **4.2.29 Test Case 2.29: Fault Notification sent via NSI (T01-02.05.07)**

This test verifies that the NSI, NASA Space Internet, transmitting a fault notification from GSFC to EDF. The fault notification will be in the form of a consistently formatted electronic message that can be automatically parsed by a receiving program from ECS. It will contain enough information to determine the nature of the fault and which sites are affected.

##### Test Inputs

The NSI schedules preventive maintenance to one of its connections to GSFC. The fault notification will contain the preventive maintenance schedule as to when the maintenance begins, ends, and to what locations are affected. In this case, the EDF is affected.

##### Test Steps

TBD

##### Test Outputs

Fault notification sent electronically as an alert. Also, the fault notification contributes to an audit trail that assist with performing network analysis.

##### Success Criteria

The fault notification will reflect all of the pertinent information users need to know.

##### Assumptions and Constraints

None.

### **4.3 System Management Thread Test**

The purpose of this thread is to verify the functionality of the Directory/Naming Service (used to uniquely associate a name with resources/principals, along with their attributes), the Distributed Time Service (DTS - used to synchronize time services across hosts located within the same DCE cell), and the HP OpenView Enterprise Management Framework (used to monitor software and hardware objects, as well as detect and display alarms).

Special resources required for this thread test include:

- Cell Directory Service Command Program (cdscp)
- XRunner
- LoadRunner
- Privileges to execute DTS management functions
- Sample science data files
- HP OpenView
- Network analyzer

#### **4.3.1 Test Case 3.1: X/Open Functions (TC004.001)**

This test case will demonstrate that the Directory/Naming Service can provide basic X/Open Federated Naming functions.

##### Test Inputs

Perform X/Open functions.

##### Test Steps

Log onto a DAAC workstation.

Create a list of directory entries.

Verify that the Directory Service determines which naming service to use from a given context.

List the names in the directory.

Get an entry from the directory.

Delete a directory.

Create attributes for a directory.

List the attributes for a directory.

Get attribute information for a directory.

Set attribute information for a directory.

Delete attribute information for a directory.

Associate a directory to attributes.

##### Test Outputs

The Directory/Naming Service should display all relative information pertaining to the above functions.

##### Success Criteria

The Directory/Naming Service should be able to perform all of the above functions.

##### Assumptions

None.

#### **4.3.2 Test Case 3.2: Replication (TC004.002)**

This test case will demonstrate that the Directory/Naming Service can provide and maintain copies of the namespace across DAAC workstations. Read/write access and propagation of master changes to replicas will also be verified.

### Test Inputs

cdscp commands

### Test Steps

Log onto a DAAC server workstation.

Using cdscp commands, create a clearinghouse (master copy).

Log onto another server workstation in the same DAAC.

From the second workstation, create a read-only copy of the clearinghouse created in step 2.

Attempt to write to a file in the replica created in step 4. CDS should prohibit this action.

Ensure that the attribute for the propagation of changes is set to "low" (no immediate skulk).

Modify a file in the master clearinghouse. These changes should not be applied to the read-only replica.

Manually propagate the file changes in step 7. These changes should now be applied to the read-only replica.

Ensure that the attribute for the propagation of changes is now set to "high" (immediate skulk).

Modify another file in the master clearinghouse.

These modifications should now be automatically applied to the read-only replica.

### Test Outputs

The Directory/Naming Service should display all relative information pertaining to the above functions.

### Success Criteria

This test will be deemed successful when the Directory/Naming Service enables one to perform all of the above functions.

### Assumptions

It is assumed that the DAAC file system will be populated with a number of directories, sub directories, data files, and other objects.

## **4.3.3 Test Case 3.3: Distribution (TC004.003)**

This test case will demonstrate that the Directory/Naming Service can distribute and manage namespaces and replicas across different hosts.

### Test Inputs

cdscp commands

### Test Steps

Using cdscp administration commands, partition a namespace in a DAAC among three different hosts.

Using cdscp administration commands, replicate partitions of this namespace across three different hosts.

Via the Global Data Service (GDS), attempt to access namespace information between two DAAC hosts.

Verify that the namespace can be updated automatically and manually.

Verify that the CSS Directory Service shall interact with the Security Service to provide host based security to the entries in the namespace.

Perform the cdscp command to denote the relative root of several namespaces.

Verify that the DCE profile function reduces search time for name lookups.

Verify that a local cache is maintained to keep recent lookup information.

### Test Outputs

The Directory/Naming Service should display all information pertaining to each replica's location. An updated namespace and a local cache maintaining the most recent lookup information to be retrieved easily.

### Success Criteria

This test will be deemed successful when the Directory/Naming Service enables one to perform all of the above functions.

### Assumptions

It is assumed that the DAAC file system will be populated with a number of directories, sub directories, data files, and other objects.

## **4.3.4 Test Case 3.4: Single Host Time Synchronization (TC005.001)**

The purpose of the single host time synchronization test is to verify that time on a given client is synchronized (within the maximum inaccuracy set) to the UTC.

### Test Inputs

Inputs to this test case include:

- DTS tuning characteristics values:

<u>Parameter</u>	<u>Default Value</u>
Maximum Inaccuracy	100 ms
Server Sync Hold Down	2 mins
Client Sync Hold Down	10 mins
Error Tolerance	10 mins
Local Set Timeout	2 secs
Global Set Timeout	15 secs
Query Attempts	3

### Test Steps

Execute an XRunner script and cron job to simultaneously get the UTC as well as the DCE time from a given host.

### Test Outputs

The expected results of this test include RPC entries with DTS time stamp.

### Success Criteria

This test will be deemed successful when UTC time and local client DCE time are synchronized.

### Assumptions

In accordance with the DCE Admin guide, time stamps retrieved are cell specific. In other words, there is no time synchronization between DCE cells. All time synchronization tests will therefore be conducted within a single DCE cell (to verify time synchronization among the hosts within that cell). The focus will be on inaccuracy verification. The test case may require the verification for other parameters.

## **4.3.5 Test Case 3.5: Multiple Host Time Synchronization (TC005.002)**

The purpose of the multiple host time synchronization test is to verify that time on multiple clients is synchronized (within the maximum inaccuracy set) to the UTC in a given DCE cell.

### Test Inputs

Inputs to this test case include:

- DTS tuning characteristics values:

<u>Parameter</u>	<u>Default Value</u>
Maximum Inaccuracy	100 ms
Server Sync Hold Down	2 mins
Client Sync Hold Down	10 mins
Error Tolerance	10 mins
Local Set Timeout	2 secs
Global Set Timeout	15 secs
Query Attempts	3

### Test Steps

Execute a LoadRunner script and cron job to simultaneously get the UTC from a given host and the DCE time from all other hosts.

### Test Outputs

The expected results of this test include RPC entries with DTS time stamp.

### Success Criteria

This test will be deemed successful if all time stamps across the DCE cell result in identical time identification within the acceptable DCE tolerances.

### Assumptions

In accordance with the DCE Admin guide, time stamps retrieved are cell specific. In other words, there is no time synchronization between DCE cells. All time synchronization tests will therefore be conducted within a single DCE cell (to verify time synchronization among the hosts within that cell).

#### 4.3.6 Test Case 3.6: Inaccuracy Injection (TC005.003)

##### Test Inputs

Inputs to this test case include:

- DTS tuning characteristics values:

<u>Parameter</u>	<u>Default Value</u>
Maximum Inaccuracy	100 ms
Server Sync Hold Down	2 mins
Client Sync Hold Down	10 mins
Error Tolerance	10 mins
Local Set Timeout	2 secs
Global Set Timeout	15 secs
Query Attempts	3

##### Test Steps

Through the DTS management functions set the drift rate on a given host to exceed the maximum allowable rate.

Execute LoadRunner script from test case 2 to capture time stamps at intervals of 15 seconds.

##### Test Outputs

The expected results of this test include DTS time displays before and after inaccuracies are introduced.

##### Success Criteria

This test will be deemed successful when the correct time within tolerance range is computed by DTS and propagated to all hosts.

##### Assumptions

At least two of the three DTSs are up and accurately running.

#### 4.3.7 Test Case 3.7: DTS Management (TC005.004)

The purpose of the DTS Management test is to demonstrate that DTS DCE services are configurable within the DTS pyramid. Clerks, Servers (local, global, couriers, backup couriers, time providers), maximum drift rates and inaccuracies, and time representation formats will be modified as part of an M&O type scenario.

### Test Inputs

Inputs to this test case include:

- DTS tuning characteristics values:

<u>Parameter</u>	<u>Default Value</u>
Maximum Inaccuracy	100 ms
Server Sync Hold Down	2 mins
Client Sync Hold Down	10 mins
Error Tolerance	10 mins
Local Set Timeout	2 secs
Global Set Timeout	15 secs
Query Attempts	3

- Commands for DTS modification

### Test Steps

dtscp

dtstd

Clerk and server startup and shutdown

Displaying and setting the time

Installing new servers

Converting clerks to servers

Identifying and fixing faulty servers

System tuning

### Test Outputs

The expected results of this test include screen displays for the DTS commands.

### Success Criteria

This test will be deemed successful when DTS management functions are demonstrated.

### Assumptions

None.

#### 4.3.8 Test Case 3.8: DTS Security (TC005.005)

The purpose of the DTS Security test is to demonstrate that security functions are invoked in the DCE cell.

##### Test Inputs

Inputs to this test case include:

- DTS tuning characteristics values:

<u>Parameter</u>	<u>Default Value</u>
Maximum Inaccuracy	100 ms
Server Sync Hold Down	2 mins
Client Sync Hold Down	10 mins
Error Tolerance	10 mins
Local Set Timeout	2 secs
Global Set Timeout	15 secs
Query Attempts	3

##### Test Steps

Exercise DTS privileges for:

- Principal
- Server Group

##### Test Outputs

The expected results of this test include screen displays for the DTS commands.

##### Success Criteria

This test will be deemed successful when DTS security functions are demonstrated.

##### Assumptions

In accordance with the DCE Admin guide, time stamps retrieved are cell specific. In other words, there is no time synchronization between DCE cells. All time synchronization tests will therefore be conducted within a single DCE cell (to verify time synchronization among the hosts within that cell).

#### 4.3.9 Test Case 3.9: DBMS Interface (TC013.003)

The purpose of the DBMS Interface test is to verify that an interface is provided to ingest the history log (flat file) into the database. Verify that the all of the desired information from the history log is ingest to the database (i.e., verify that each entries logged into the flat file contains all of the appropriate information: application start or stop time, application name/version, event message information, event message type, event disposition narrative, user principle information,

and environment information). Verify that the PMAS provides the queries to generate performance reports.

### Test Inputs

Inputs to this test case include history log files created from each of the available DAACs and from the EDF. Inputs to this history log file include a series of system logins, file transfers using FTP and RPC for a given data file, activation, execution, termination of other application software provided as part of IR-1, and performance data. Generated queries.

### Test Steps

Tester will login to the IR-1 application using a valid id and valid password, an invalid id and valid password, a valid id and invalid password and an invalid id and valid password

Tester will implement the available applications (making sure for each application started, it will also be closed) to make entrants into the history log

Tester will set a threshold and run a test that will surpass the threshold.

Verify that the history log will record the event via the CSS implemented API.

Simulate the retrieval of the science algorithm performance data from the local History Logs using the CSS provided APIs.

Tester will switch to the history log directory.

Ingest the history log into the database.

Verify the desired information from the history log is entered into the database.

Verify that the PMAS provides queries to generate performance statistics from the performance data stored in the database.

Verify that network statistics for a configurable period of time for performance data store in the management database (average, median, maximum, minimum, ratios, rates and standard deviations).

Verify that the generated performance data is stored in the PMAS.

Print the M&O staff selected performance statistics, via the PMAS.

### Test Outputs

The expected results of this test include:

An entry in the history log for each login attempt (valid or invalid) and a time stamp of when the action occurred.

An entry for the activation of the application with a corresponding start time and an entry for the termination of the application with a corresponding stop time.

An entry for the crossing of a threshold.

Science Algorithm performance data from the History Logs.

A database that maintains all of the desired information from the history log file.

Reports based on the results of the PMAS provided queries.

Stored performance data within the PMAS.

A printout of the M&O staff-selected performance statistics.

#### Success Criteria

This test will be deemed successful when the history log is ingested to the database and the information in the history log corresponds to the information in the database.

#### Assumptions and Constraints

None.

### **4.3.10 Test Case 3.10: Management Data Access (TC013.004)**

The purpose of the management data access test is to verify that a user can schedule the transfer and loading of the log files and an application can load the files into the management database. Verify that the database is accessible and that the integrity of the management data is maintained.

#### Test Inputs

Inputs to this test case include: management data, setting up a schedule to transfer and loading of the log files.

#### Test Steps

Access management data (verify that CSS services were used)

Transfer management data (verify that CSS Services were used)

Using an application access the management data

Repeat above step for selective data

Schedule the transfer and loading of log files

When the scheduled time is reached verify that the log files were transferred and loaded

Using an application verify that you can load the log files

Verify that throughout all of the above steps the data integrity was maintained

#### Test Output

Outputs to this test case include: Accessed and transferred management data, selectively accessed data and loaded log files.

### Success Criteria

This test will be deemed successful when data has been transferred and loaded using both predetermined schedules and an application, log files were loaded and the integrity of the data was maintained.

### Assumptions and Constraints

None.

#### **4.3.11 Test Case 3.11: Performance Monitoring Thresholds (TC013.005)**

The objective of this test case is to demonstrate the ability of the MSS Performance Management Application Service to provide a number of configurable thresholds for each performance metric, provide default values, allow for the modification of these values, and compare received values against these thresholds.

- **Memory Threshold Fault**

This test verifies that the HP OpenView Network Node Manager detects and locates the computer with the memory threshold fault. Since most computers utilize a portion of their hard disk as virtual memory, the Management Information Base object created to monitor a computer's memory will contain threshold limits to determine when the memory capacity of a computer is in excessive use. (Test will be verified on all workstations/PCs at each site.)

- **CPU Threshold Fault**

This test verifies that the HP OpenView Network Node Manager detects and locates the computer where the CPU threshold limit has been exceeded. The Management Information Base object created will contain threshold limits to determine when the CPU load of a computer is in excessive use. (Test will be verified on all workstations/PCs at each site.)

- **Hard Disk Capacity Fault**

This test verifies that the HP OpenView Network Node Manager detects and locates the computer with a storage capacity fault. To simulate full capacity on a storage device, the tester will store large postscript or HDF files to the storage device. This test is limited to workstations and PCs with less than 1 GB of storage. (Test will be verified on all workstations/PCs at each site.)

### Test Inputs

Inputs to this test case include HP OpenView Network Node Manager commands and ECS performance data.

A list of initial thresholds, including memory and CPU threshold limits.

Root map of the HP OpenView Network Node Manager window will be active in the tester's display.

### Test Steps

Verify that the PMAS provides a configurable number of thresholds for each performance metric.

Verify that the EMC PMAS can create and send a list of suggested initial thresholds for each performance metric to the MSS site performance management application via CSS services and that the sites can receive it.

Examine the above list to ensure that a suggested initial threshold value exists for each performance metric.

Execute an application that exceeds the memory threshold limit determined within the Management Information Base object created to monitor the computer memory usage. (If threshold limit is too high to exceed, lower the threshold as needed. After test, threshold limit will be returned to original state.)

Execute an application that utilizes all/most of the CPU processing time.

Store as many large postscript and HDF files to the system storage device as possible without damaging any existing files on the system.

Ensure that the proper alarms/warning have been disseminated concerning any values exceeding their thresholds.

Reconfigure these threshold values to higher settings.

Reconfigure these threshold values to lower settings.

### Test Outputs

Proper alarms/warning have been disseminated concerning any values exceeding their thresholds.

Internet symbol on Root map of the HP OpenView Network Node Manager window has turned YELLOW.

Traversing through the Internet submaps, following the YELLOW/marginal status symbols, the tester should be directed to the computer (indicated by color of RED) that contains the memory threshold fault, where the CPU threshold limit has been exceeded, or that contains the storage device fault (a message indicating storage capacity should also be displayed).

### Success Criteria

This test will be deemed successful when all performance parameters exceeding their configured thresholds are flagged.

### Assumptions and Constraints

None.

#### **4.3.12 Test Case 3.12: Basic Monitoring (TC014.001)**

The purpose of the Basic Monitoring test is to demonstrate the management frameworks ability to create and display graphical representations of network topologies and to organize the given network topology into a hierarchy of maps.

- DAAC Hardware Confirmation

This test verifies that the HP OpenView Network Node Manager properly detects and monitors all hardware located at the local sites (GSFC, MSFC, LaRC, and the EDF).

- DAAC Software Process Monitoring

This test verifies that the MIB created within the HP OpenView Network Node Manager properly monitors all software processes at the local sites (GSFC, MSFC, LaRC, and the EDF).

- Generation, Collection, Storing, and Displaying of Network Statistics

This test verifies that the HP OpenView Network Node Manager is able to generate, collect, store, and display network statistics.

##### Test Inputs

Inputs to this test include the SNMP (the ECS standard protocol as specified in RFC 1157) managed objects.

Local site submap of HP OpenView Network Node Manager is active in the tester's display. Contact site liaisons and receive a list of all hardware components and software processes that are active, in-use, and should be monitored.

Request to display network statistics for GSFC, MSFC, LaRC & EDF systems.

##### Test Steps

Initialize HP OpenView and verify that a map depiction of the network topology is accurately displayed

Verify that the lower level topologies include hosts, routers, network interface cards, bridges, gateways, operating systems, peripherals, databases and there status.

Double click on the available icons to verify that lower level submaps exist

Determine the operational state of all network components, hosts and peripherals.

Force an operational state of a network component to change (repeat for hosts, applications and peripherals).

Demonstrate the ability of the PMAS to receive notification of the change.

Demonstrate the capability of the PMAS to monitor the performance of network components (repeat for hosts, operating systems, peripherals, and databases).

Demonstrate the capability of the performance management application service to monitor ECS component protocol stack performance parameters and Ethernet-like device performance parameters as defined in IETF RFC 1213 and IETF RFC 1623, respectively.

Repeat above steps locally at each site.

#### Test Outputs

Local site submap of HP OpenView Network Node Manager displays all hardware active at each site. Listing of all hardware and software processes active and in-use at each site.

Network statistics are displayed and stored for GSFC, MSFC, LaRC & EDF systems.

#### Success Criteria

Hardware and software processes displayed in local site's submap of HP OpenView Network Node Manager matches/confirms hardware and software processes that is obtained from the site liaison.

#### Assumptions and Constraints

None.

### **4.3.13 Test Case 3.13: OpenView (TC014.002)**

The purpose of the OpenView test is to demonstrate the accuracy in which OpenView can monitor the changes that take place over the network and its ability to notify the Systems Administrator. The following series of tests verifies that OpenView will properly detect and locate hardware faults (computer, gateway/router, printer, peripheral, etc.) that are connected within the LAN/WAN network. Hardware faults may be caused by power loss or a network disconnect. The tests will also verify that OpenView will properly detect and locate software application initialization and termination, as well as perform protocol testing. All events should be recorded in a problem log.

#### Test Inputs

Inputs to this test case include initialization/termination of a software application that is being monitored by SNMP (Simple Network Management Protocol), hardware power loss and hardware connection/disconnection from the network.

#### Test Steps

Log onto a workstation, and initialize HP OpenView.

Verify that all objects/applications that are being monitored by SNMP are visible from the display.

Initialize an application being monitored by OpenView, and verify that the system recognizes the monitoring of the application.

Exit from the application, and verify that the system depicts the change.

Verify that OpenView can perform an IP protocol test.

Verify that OpenView can perform an TCP protocol test.

Verify that OpenView can perform an SNMP protocol test.

Verify that OpenView can perform an UDP protocol test.

Verify that OpenView can perform an ICMP protocol test.

Connect a hardware device (e.g. printer) to the network and verify that the system recognizes the new configuration.

Turn off the power to the hardware device (e.g. computer, gateway/router) and verify that the system recognizes the new configuration.

Turn the power to the hardware device back on and verify that the system recognizes the new configuration.

Disconnect the hardware device from the network and verify that the system recognizes the new configuration.

Change to the directory which contains the history log.

Examine the history log to determine whether all appropriate events have been documented.

Verify that with all of the network changes that occur an E-mail message was sent to the System Administrator.

#### Test Outputs

The expected results of this test include both visual and E-mail notification to the System Administrator. The history log file will be analyzed to determine that all network changes were logged properly.

#### Success Criteria

This test will be deemed successful when all network changes have been detected and logged and the Systems Administrator notified for each change as part of the dialog session.

#### Assumptions and Constraints

None.

#### **4.3.14 Test Case 3.14: Fault Indication (TC014.003)**

The objective of the Fault Indication test is to determine if a fault is categorized into proper severity levels.

- Multi-Process Termination Fault

This test verifies that the HP OpenView Network Node Manager detects and locates the computer and processes that have been abruptly terminated. In this test many processes will be activated (GUIs, ftps, etc..), then some of the processes will be abruptly 'killed' simulating failures. Sample processes to kill include SNMP agents, DCE servers, ECS servers, etc..

##### Test Inputs

Inputs to this test case include setting the degree of a fault and modifying the time frame in which data will be gathered.

Root map of the HP OpenView Network Node Manager window will be active in the tester's display.

##### Test Steps

Initialize OpenView

Set the fault category for a particular fault

Re-configure the time in which the data will be gathered

Activate many processes on a host machine. (FTP's, Telnet, GUIs, etc.) 'Kill' a quarter of the processes from the machine.

Monitor the activity to verify that the system has accepted the changes

Display the information stored in the OpenView file

##### Test Outputs

The expected outputs include a display of the data gathered at the times indicated.

Internet symbol on Root map of the HP OpenView Network Node Manager has turned YELLOW.

Traversing through the Internet submaps, following the YELLOW/marginal status symbols, the tester should be directed to the computer and processes that were terminated.

##### Success Criteria

This test will be deemed successful when the fault categories we set have been implemented and the information is gathered for the predetermined times.

##### Assumptions and Constraints

None.

#### **4.3.15 Test Case 3.15: MUI Services (TC014.004)**

The purpose of the MUI (Management User Interface) Services test is to verify that the MUI Service provides all of the desired capabilities.

##### Test Inputs

Inputs to this test case include mouse and keyboard inputs, adding, deleting and modifying of symbols (shape, color and position), add, delete and modification of text string, M&O screen configuration changes, staff alert, vendor MIBs, managed objects and managed applications.

##### Test Steps

Initialize OpenView.

Launch an Xterm from the MUI to establish a dialog session with the M&O staff.

Demonstrate the MUI services compatibility with the ECS management framework.

Inspect the MUI to verify compliance with OSF/MOTIF.

Demonstrate using keyboard and mouse inputs the MUI service capability to respond.

Verify the capability of the M&O staff and an application to add/delete a symbol and modify the shape, color and position of the symbol.

Demonstrate the capability of the M&O staff and an application to add/delete and modify text strings.

Acting as an M&O user, verify that you can make screen configuration changes and save these changes.

Verify that as both M&O and an application you can load and unload vendor MIBs.

Verify that an M&O user has the capability to register and unregister managed objects and management applications.

Verify capability to configure/customize event notifications.

Verify that the MUI provides on-line help windows for the applications.

Verify that the PMAS is capable of graphically displaying the operational state of managed objects in graphical form via the MUI service.

Verify that the PMAS is capable of displaying M&O staff-selected performance statistics in graphical and tabular form through the MUI service.

Print the performance statistics.

##### Test Outputs

Outputs to this test case include: responses from the MUI to the keyboard and mouse inputs, additions, deletions and modifications of symbols, add, delete and modification of text strings, new screens upon configuration changes, vendor MIBs, managed objects and management

applications and on-line help windows. Graphical displays of the operational states of managed objects and graphical and tabular displays of M&O staff-selected performance statistics. A printout of the performance statistics.

#### Success Criteria

This test will be deemed successful when all of the represented test steps have been executed and the appropriate results were obtained.

#### Assumptions and Constraints

None.

### **4.3.16 Test Case 3.16: Performance Management (TC014.005)**

The purpose of the Performance Management test is to verify that all of the documented capabilities and requirements are tested and verified.

#### Test Inputs

Inputs to this test case include: managed objects, performance metrics and requested performance data.

#### Test Steps

Demonstrate the ability of the PMAS to manage an object.

Verify that the PMAS is capable of receiving managed object definitions for each managed object.

Gather data for various performance metrics from each individual managed object, verify that you are able to specify which metrics you would like to gather.

Demonstrate the ability of the PMAS to request data from the individual managed objects on a configurable interval and on demand.

Verify that the PMAS can receive requested performance data from the ECS components.

Demonstrate the ability of the PMAS to retrieve data for all hosts, peripherals and network component interfaces.

#### Test Outputs

Reports of performance metrics, requested data from individual objects, requested performance data.

#### Success Criteria

This test will be deemed successful when the PMAS meets all of the functionality outlined above.

#### Assumptions and Constraints

None.

#### **4.3.17 Test Case 3.17: Monitor/Control and Management Agent (TC014.006)**

The purpose of the Monitor/Control and Management Agent test is to verify the functionality provided by the Management Agent Service and the Monitor/Control Service, as well as their ability to interact with each other.

##### Test Inputs

Inputs to this test case include: ECS management set messages, traps/events, performance and fault data, data from ECS managed objects, and a proxy agent for ECS network devices.

##### Test Steps

Demonstrate the communications via the ECS management protocol between the Monitor/Control Service and the Management Agent Service in test or operational mode.

Verify that the Monitor/Control Service can send ECS management set messages to configure and control the processing performed by the ECS management agent and receive ECS management traps/events.

Demonstrate the functionality associated with the Monitor/Control Service to perform statistical analysis on the performance and fault data collected from the Management Agent Service.

Verify that the MSS Management Agent Service retrieves data from ECS managed objects in test or operational mode.

Verify that the Management Agent Service can respond to requests for managed object MIB attributes.

Verify the capability to browse MIB values.

Verify that the Management Agent Service can receive ECS management traps/events and set messages from the Monitor/Control Service.

Demonstrate the ability of a Management Agent Service provided ECS management agent to be configurable to include: community to respond to and set attributes, agent location and contact person, traps to send and events to log and log file name.

Verify that an ECS management agent is provided for network devices.

Verify that for all network devices and applications, which can not be managed via SNMP, the Management Agent Service provides proxy agents.

##### Test Outputs

Outputs to this test case include, but are not limited to: communications between the Monitor/Control Service and Management Agent service, management traps/events, statistical analysis, retrieved data from the ECS managed objects, a configured management agent and proxy agents.

#### Success Criteria

This test will be deemed successful when communications between the Management Agent Service and Monitor/Control Service and all of the documented functionality has been verified.

#### Assumptions and Constraints

None

#### **4.3.18 Test Case 3.18: Problem Tracking Test (TS002.011)**

This test case demonstrates the ability to track problems that are identified in the configured Ir-1 environment.

#### Test Inputs

Inputs to this test are simulated problems found in the Ir-1 environment.

#### Test Steps

TBD

#### Test Outputs

Outputs to this test are Problem Tracking reports.

#### Success Criteria

This test is deemed successful if all simulated problems found in the Ir-1 environment are tracked and problem reports are generated.

#### Assumptions and Constraints

None

#### **4.3.19 Test Case 3.19: Remote NCR (BC016.003)**

This test case demonstrates the capability of a user at a DAAC to log a NCR (Non conformance Report).

#### Test Inputs

Inputs to this test case include the submittal of an NCR by a user located at one of the DAACs.

#### Test Steps

Have the system administrator create a test account on one of the DAACs.

Log into the DAAC as that user.

Using the Discrepancy Tracking System document a discrepancy.

Verify that the NCR is logged.

Verify that appropriate E-mail notifications are sent out through DDTS.

Track the progress of the NCR through verification.

#### Test Outputs

The expected results of this test include the ability of a DAAC user to record an NCR into the Discrepancy Tracking System. A printout documenting the discrepancy should be generated.

#### Success Criteria

This test will be deemed successful when a user located at the DAAC can log a discrepancy report and track the success of solving the discrepancy.

#### Assumptions and Constraints

None.

### **4.3.20 Test Case 3.20: Hardware Monitoring Process Terminated (T04-01.01.06)**

This test verifies that the System Management Framework tool will detect and locate a hardware "fault" when the monitoring process of the specific piece of hardware has been terminated. Testing includes monitoring the System Management Framework tool while the monitoring process is terminated, therefore, a System Management Framework window will be displayed on the workstation/PC where the tester is located. (Test will be verified at each site.)

#### Test Inputs

Root map of System Management Framework window will be active in the tester's display. Tester will locate and terminate/"kill" the process that monitors the hardware.

#### Test Steps

TBD

#### Test Output

Internet symbol on Root map of System Management Framework has turned YELLOW.

#### Success Criteria

Traversing through the Internet submaps, following the YELLOW/marginal status symbols, the tester should be directed to the "faulty" piece of hardware (indicated by color RED).

#### Assumptions and Constraints

None.

### **4.3.21 Test Case 3.21: Gateway/Router Monitoring Process Terminated (T04-01.01.09)**

This test verifies that the System Management Framework tool detects and locates a possible fault with a gateway/router. Testing includes displaying the System Management Framework tool, while the tester terminates the process that monitors the gateway/router activities. (Test will be verified at each site.)

#### Test Inputs

Root map of System Management Framework window will be active in the tester's display. Tester will locate and "kill" the process that monitors the gateway/router.

#### Test Steps

TBD

#### Test Output

Internet symbol on Root map of System Management Framework has turned RED.

#### Success Criteria

Traversing through the Internet submaps, following the RED/critical status symbols, the tester should be directed to the faulty gateway/router (color should be RED).

#### Assumptions and Constraints

None.

### **4.3.22 Test Case 3.22: Software Application Monitoring Process Termination (T04-01.01.12)**

This test verifies that the System Management Framework tool detects and locates the terminated software application when the monitoring process of the application has been terminated. Testing includes monitoring the System Management Framework tool while the monitoring process is terminated, therefore, a management window will be displayed on the workstation/PC where the tester is located. (Test will be verified at each site.)

#### Test Inputs

Root map of System Management Framework window will be active in the tester's display. Tester will locate and terminate/"kill" the process that monitors the software application.

#### Test Steps

TBD

#### Test Output

Internet symbol on Root map of System Management Framework has turned YELLOW.

#### Success Criteria

Traversing through the Internet submaps, following the YELLOW/marginal status symbols, the tester should be directed to the computer where the application was running (computer will be RED in color) and the application itself.

#### Assumptions and Constraints

None.

#### **4.3.23 Test Case 3.23: Computer Monitoring Process Terminated (T04-01.01.18)**

This test verifies that the System Management Framework tool will detect and locate a computer "fault" when the monitoring process of the computer has been terminated. Testing includes monitoring the System Management Framework tool while the monitoring process is terminated, therefore, a System Management Framework window will be displayed on the workstation/PC where the tester is located. (Test will be verified at each site.)

##### Test Inputs

Root map of System Management Framework window will be active in the tester's display. Tester will locate and terminate/"kill" the process that monitors the computer.

##### Test Steps

TBD

##### Test Output

Internet symbol on Root map of System Management Framework has turned YELLOW.

##### Success Criteria

Traversing through the Internet submaps, following the YELLOW/marginal status symbols, the tester should be directed to the "faulty" computer (indicated by color or RED).

##### Assumptions and Constraints

None.

#### **4.3.24 Test Case 3.24: Operating System Monitoring Process Terminated (T04-01.01.20)**

This test verifies that the System Management Framework tool detects and locates the computer with the "failed" operating system. To simulate a failed operating system the monitoring process of the system will be terminated/"kill"ed, no processing will be harmed. Testing includes monitoring the System Management Framework tool while the monitoring process is terminated. (Test will be verified on all computers at each site.)

##### Test Inputs

Root map of System Management Framework window will be active in the tester's display. Opening an xterm window from a host machine, locate and "kill" the process that monitors the operating system.

##### Test Steps

TBD

##### Test Output

Internet symbol on Root map of System Management Framework has turned YELLOW.

#### Success Criteria

Traversing through the Internet submaps, following the YELLOW/marginal status symbols, the tester should be directed to the computer and actual operating system fault that occurred (Computer will be RED in color).

#### Assumptions and Constraints

None.

### **4.3.25 Test Case 3.25: Local Site Management/Security Policy and Procedures (T04-01.02.03)**

This test verifies that local site security policy & procedures including password management, operational security, data classification, compromise mitigation and access/privileges, systems hardware and software maintenance, and spares inventory guidelines are current and updated at each site supported by this release.

#### Test Inputs

Security management policies and procedures.

#### Test Steps

TBD

#### Test Output

Security management policies and procedures from GSFC, MSFC, and LaRC.

#### Success Criteria

Security sections within all documents are current and identical to that copy held at the EDF.

#### Assumptions and Constraints

None.

### **4.3.26 Test Case 3.26: Active DAAC ECS Administrator Account (T04-01.05.01)**

An active Administrator account exists to provide a maintenance and operational interface to the DAACs to allow resource usage and management.

#### Test Inputs

Account with special accesses assigned to System Administrator.

#### Test Steps

TBD

#### Test Output

Account exists with necessary privileges.

#### Success Criteria

Interface account for system exists.

#### Assumptions and Constraints

None.

### **4.3.27 Test Case 3.27: ECS Software Backup Maintained (T04-01.05.02)**

A minimum of one backup save set is maintained in a separate physical location of the ECS software.

#### Test Inputs

Management policies and procedures guidelines from the EDF.

#### Test Steps

TBD

#### Test Output

Management policies and procedures manual from GSFC, MSFC, and LaRC.

#### Success Criteria

Section within document are current and identical to that copy held at the EDF.

#### Assumptions and Constraints

None.

### **4.3.28 Test Case 3.28: Monitoring and Replenishment of Spares Inventory (T04-01.05.03)**

Verify the monitoring of usage and replenishment of the computer paper, tapes, disks inventory. Guidelines are defined in the Policies and Procedures Manual.

#### Test Inputs

Management policies and procedures guidelines from the EDF.

#### Test Steps

TBD

#### Test Output

Management policies and procedures manual from GSFC, MSFC, and LaRC.

#### Success Criteria

Section within document are current and identical to that copy held at the EDF.

## 4.4 System Administration Build Test

The System Administration Build Test represents an aggregation of the DCE Infrastructure, Messaging and File Transfer, and System Management Threads. The functions to be tested include general DCE functionality, network management, fault management, security management, and Ir-1 internetworking capabilities.

Special resources required for this thread test include:

- Cell Directory Service Command Program (cdscp)
- XRunner
- LoadRunner
- Privileges to execute DTS management functions
- Sample science data files
- HP OpenView
- Network analyzer

### 4.4.1 Test Case 4.1: General DCE (BC008.001)

The purpose of the General DCE test is to demonstrate, that upon integration of the custom code developed for the DCE Infrastructure, Messaging and File Transfer, and System Management Threads, all of the expected capabilities will remain intact.

#### Test Inputs

Inputs to this test case include a valid ID and valid password, various combinations of valid/invalid ID and valid/invalid password, valid admin ID and password, valid add, change and delete registry commands, ability to access and modify directories, time checks using DTS.

#### Test Steps

Run an XRunner script to execute a number of login attempts using a combination of valid/invalid IDs and passwords.

Upon successful login, call another XRunner script to change the users password, logout and login with the new password

Create a cron job that will logon to each of the available IR1 workstations and record the distributed time in a flat file

Start the cron job running in the background

Logon as the DCE Administrator

Add, change, and delete commands to/from the security registry

Set up a cron job to retrieve the time from each of the workstations in the IR1 operational cell and store them in a file

Inspect the file to insure that all of the times are in sync

Set up a workstation to run as the server

Set up all of the workstations to be clients (including the server workstation)

Initialize the server

Initialize communications between client and server.

View the flat file containing the times from the various workstation to ensure distributed time

#### Test Outputs

Screen outputs showing the success or failure of the logon/logoff attempts. Response times of each logon and logoff event. Network monitor output showing the data transmitted between client and server. Event log data. Flat file showing the times recorded during execution of the cron job. Screen outputs showing successful bindings between clients and server.

#### Success Criteria

The test will be deemed successful when all IR1 DCE functionality have been demonstrated and verified.

#### Assumptions

None.

### **4.4.2 Test Case 4.2: Network Management Test (BC002.004)**

This test case demonstrates that the internetworking devices do event notification of relevant networking events.

#### Test Inputs

Network manager commands to activate network device agents.

#### Test Steps

Run network benchmarks with network event logging turned on.

Use network manager to requests various types of event data from network devices.

Introduce anomalies into the system, for example causing the failure or interruption of various network devices.

Repeat above steps for a software configurable item.

#### Test Outputs

Logs and alarms showing recorded event data.

#### Success Criteria

Log and alarm data consistent with the above Steps. No spurious alarm or log data.

#### Assumptions

This functionality will be further verified in other build/thread tests since internetworking will implicitly be a part of most other tests.

#### **4.4.3 Test Case 4.3: Fault Management (T04-01.02.01)**

This test verifies that the fault management policies and procedures located at GSFC, MSFC, and LaRC are current and up-to-date with the current at the EDF.

##### Test Input

Current fault management policies and procedures from the EDF. Fault management policies and procedures from GSFC, MSFC, and LaRC.

##### Test Steps

TBD

##### Test Output

Fault management policies and procedures from GSFC, MSFC, and LaRC.

##### Success Criteria

Fault sections within all documents are current and identical to that copy held at the EDF.

##### Assumptions and Constraints

None.

#### **4.4.4 Test Case 4.4: Security Management (T04-01.02.02)**

This test verifies that the security management policies and procedures located at GSFC, MSFC, and LaRC are current and up-to-date with the current from the EDF.

##### Test Inputs

Security management policies and procedures from the EDF.

##### Test Steps

TBD

##### Test Output

Security management policies and procedures from GSFC, MSFC, and LaRC.

##### Success Criteria

Security sections within all documents are current and identical to that copy held at the EDF.

##### Assumptions and Constraints

None.

#### **4.4.5 Test Case 4.5: Access to GSFC (T01-02.02.02)**

This test verifies that all host machines connected to the LAN at GSFC are accessible through the network from the EDF.

##### Test Inputs

Listing of all machines connected to GSFC LAN. "ping" all host machines on listing.

##### Test Steps

Log onto V0 host machine.

Ping statistics from V0 host machine.

##### Test Outputs

Ping statistics displayed for each machine.

##### Expected Results

All host machines listed from GSFC should return ping messages that are connected to GSFC LAN. History log will record all activities.

#### **4.4.6 Test Case 4.6: Access to LaRC (T01-02.02.03)**

This test verifies that all host machines connected to the LAN at LaRC are accessible through the network from the EDF.

##### Test Inputs

Listing of all machines connected to LaRC LAN. "ping" all host machines on listing.

##### Test Steps

Log onto V0 host machine.

Ping statistics from V0 host machine.

##### Test Outputs

Ping statistics displayed for each machine.

##### Expected Results

All host machines listed from LaRC should return ping messages that are connected to LaRC LAN. History log will record all activities.

#### **4.4.7 Test Case 4.7: Access to MSFC (T01-02.02.04)**

This test verifies that all host machines connected to the LAN at MSFC are accessible through the network from the EDF.

##### Test Inputs

Listing of all machines connected to MSFC LAN. "ping" all host machines on listing.

##### Test Steps

Log onto V0 host machine.

Ping statistics from V0 host machine.

##### Test Outputs

Ping statistics displayed for each machine.

##### Expected Results

All host machines listed from MSFC should return ping messages that are connected to MSFC LAN. History log will record all activities.

#### **4.4.8 Test Case 4.8: Internetworking Test (BC002.002)**

This test case tests internetworking services for TCP/IP and UDP/IP over Ethernet and FDDI, and verifies POSIX compliance on UNIX platforms.

##### Test Inputs

Benchmark internetworking test data.

##### Test Steps

Run internetworking benchmark test suite for TCP/IP and UDP/IP protocols.

Inspect POSIX certifications, compiler settings, etc.

##### Test Outputs

Comparisons of test data sent and received, network analyzer outputs, log data indication performance and fault data, and network manager alarms.

##### Success Criteria

Data successfully transported through the network, performance data consistent with prior and standard benchmark results, no anomalous performance or fault log or alarm events.

##### Assumptions

This functionality will be further verified in other build/thread tests since internetworking will implicitly be a part of most other tests.

## Appendix A. Test Tool Descriptions

The following matrix gives a listing and description of available test tools.

TOOL TYPE	SELECTED TOOL	TOOL DESCRIPTION
Configuration Management Tool	ClearCase	Developed by Atria Software, Inc. Uses VOBs (Version Object Base) to store the software versions. A VOB is a virtual directory tree of sources and other objects and is mounted like a disk partition. A project may have many VOBs. Any changes made by the developer after the software has been frozen will be conducted on a branch. The test organizations are responsible for merging the fixes (branches).
Non Conformance Reporting Tool:	DDTS	Distributed Defect Tracking System (DDTS) developed by QualTrak Corporation. DDTS is a UNIX change management and bug tracking system that tracks and manages changes tracks and manages changes throughout the life cycle of a hardware or software product from initial requirements planning obsolescence in the field. DDTS was specifically designed to aid developers during product development and the quality assurance organization during the testing phase. This tool works hand and hand with ClearCase
Capture and Playback Tool	XRunner	XRunner was developed by Mercury Interactive Corporation. XRunner is an advanced automated software testing system for X window applications. XRunner automates the full range of software testing needs. Some of the gained functionality include: output synchronization, text recognition and a high-level testing mode that operates directly on GUI objects.
Automated Client/Server Testing System	LoadRunner	LoadRunner is developed by Mercury Interactive Corporation. It is an automated testing system for client/server applications on UNIX/X platforms. By running multiple users in parallel off the server, LoadRunner enables us to automate load testing, performance testing and system tuning.
Requirements Traceability Tool	RTM	Requirements & Traceability Management tool is developed by GEC-Marconi Limited configurable to support our methodology. RTM provides an audit trail that will enable us to trace various requirements. The tool is driven by requirements and provides an easy avenue for the production of requirements related documents or matrix.
Network Management Framework	OpenView	OpenView is developed by Hewlett Packard. It is a Network Management Framework. The Framework can be used to monitor any device that supports the Simple Network Management Protocol (SNMP). This tool will aid us in determining the status of the network and devices on the network.

This page intentionally left blank.

## Appendix B. Verification Traceability Matrix

The following matrix provides a mapping of Level 4 requirements to Build/Test case.

req_source_id	release	text	test_id	Verif_Method
C-CSS-00040	A   IR1	The CSS services shall be compatible with POSIX-compliant Unix platforms.	BC002.002	Inspect
C-CSS-00500	A   IR1	The CSS client services software shall be made available in the form of a CSS toolkit to the developers.	TC003.001 TC009.004 TC011.001 TC011.002 TC013.003	Test / Inspect
C-CSS-21000	A   IR1	The CSS Security service shall provide an API to verify the identity of users.	TC003.005	Test
C-CSS-21020	IR1	The CSS Security service shall provide the capability to create/modify/delete user accounts and privileges in the security registry.	TC003.005	Demo
C-CSS-21030	IR1	The CSS Security service shall provide the capability to define/modify/delete group information in the security registry.	TC003.005	Demo
C-CSS-21100	IR1	The CSS Security service shall provide an API to challenge the client/server to authenticate itself at the following three levels. a. connect level b. request level c. packet level	TC003.005	Test
C-CSS-28000	IR1	CSS Event Logger Service shall provide capability to record event and history data to a application specific log file.	TC013.003	Test
C-CSS-28010	IR1	CSS Event Logger Service shall accept and record event time (when the event was generated, obtained from the Time Service) information.	TC013.003	Test
C-CSS-28020	IR1	CSS Event Logger Service shall accept and record the application information (name and version of the calling application).	TC013.003	Test
C-CSS-28030	IR1	CSS Event Logger Service shall accept and record event message information.	TC013.003	Test
C-CSS-28040	IR1	CSS Event Logger Service shall accept and record the event type information. (Type of the event: fault, performance)	TC013.003	Test

req_source_id	release	text	test_id	Verif_Method
C-CSS-28060	A   IR1	CSS Event Logger Service shall inform M&O staff if the event disposition narrative by the application demands so.	TC013.003 TC013.004	Demo
C-CSS-28070	A   IR1	CSS Event Logger Service shall record the operator/principle information that is relevant for the generated event.	TC013.003	Test
C-CSS-28080	A   IR1	CSS Event Logger Service shall record the environment information for the generated event.	TC013.003	Test
C-CSS-60500	IR1	The CSS File Access Service shall provide functionality for interactive and non-interactive transfer of files (send and receive) between two host systems.	TC009.002	Test
C-CSS-60510	IR1	The CSS File Access Service shall be capable of transferring ASCII and binary files.	TC009.002	Demo
C-CSS-60520	IR1	The CSS File Access Service shall support the File Transfer Protocol (FTP).	TC009.001	Demo
C-CSS-60600	IR1	The CSS File Access Service shall provide connection oriented operation for file transfers.	TC009.001	Demo
C-CSS-60610	IR1	The CSS File Access Service shall allow selection of the file type (ASCII or binary).	TC009.002 TC009.004	Demo
C-CSS-60620	IR1	The CSS File Access Service shall support proxy mode of operation which enables transfer of files between two remote hosts.	TC009.002	Demo
C-CSS-60630	IR1	The CSS File Access Service shall provide capability to list remote files	TC009.001	Demo
C-CSS-60640	IR1	The CSS File Access Service shall support wildcards in files on the remote host.	TC009.001	Demo
C-CSS-60650	IR1	The CSS File Access service shall support anonymous FTP which allows read access to all users.	TC009.003	Demo
C-CSS-61040	IR1	The CSS Electronic Mail Service shall provide translation between SMTP and X.400 protocol.	TC006.001 TC006.002 TC010.001 TC010.003 TC010.004	Demo
C-CSS-61050	A   IR1	The CSS Electronic Mail Service shall be accessible in interactive mode.	TC006.001 TC006.002 TC010.001 TC010.002 TC010.003 TC010.004	Demo

req_source_id	release	text	test_id	Verif_Method
C-CSS-61060	A   IR1	The CSS Electronic Mail Service shall be accessible in non-interactive mode via API.	TC006.001 TC006.002 TC010.001 TC010.002 TC010.003 TC010.004	Test
C-CSS-63000	A   IR1	The CSS Virtual Terminal shall provide a virtual device which hides the physical terminal characteristics and handling conventions from both the operator and the server host.	TC003.001	Demo
C-CSS-63010	A   IR1	The CSS Virtual Terminal shall provide means to enhance characteristics of the basic virtual device by mutual agreement between the two communicating parties (option negotiations).	TC003.001	Demo
C-CSS-63020	A   IR1	The CSS Virtual Terminal shall be based on industry standard and accepted protocols (telnet and ktelnet).	TC003.001	Demo
C-CSS-63040	A   IR1	The CSS Virtual Terminal shall provide guest access to non-registered users to log into the ECS guest server.	TC003.001	Demo
C-HRD-23115	A   IR1	The Bulletin Board Server processor shall have the capability to support a POSIX compliant IEEE 1003.1 operating system (UNIX).	BC012.004	Demo / Inspect
C-HRD-23300	A   IR1	The Bulletin Board Server data storage shall be compatible with POSIX compliant operating systems from several vendors.	BC012.004	Demo / Inspect
C-ISS-01000	A   IR1	The ISS shall interoperate with the V0 Wide Area Network to provide IR-1 connectivity as specified in DID 220, "Communications Requirements for the ECS project".	BC002.001 BC002.002	Demo
C-ISS-01010	A   IR1	The ISS shall provide an interface between the V0 WAN and the MSFC, LaRC and GSFC DAACs for the purpose of IR-1 interface testing.	BC002.001 TC001.001	Test

req_source_id	release	text	test_id	Verif_Method
C-ISS-01020	A   IR1	The ISS shall interface with NSI or an alternate Internet provider at GSFC, MSFC, LaRC and EDC to provide DAAC access to science users in accordance with the following documents: a. DID 220, "Communications Requirements for the ECS Project" 194-220-SE3-001 b. Interface Requirements Document between EOSDIS Core System (ECS) and the NASA Science Internet (NSI), 194-219-SE1-001	BC002.001 TC001.001	Demo
C-ISS-01030	IR1	The ISS shall provide for connectivity between the MSFC DAAC and NOLAN for the ingest of L0 LIS data.	BC002.001 TC001.001	Test
C-ISS-01040	IR1	The ISS shall provide for connectivity between the LaRC DAAC and NOLAN for the ingest of L0 CERES data.	BC002.001 TC001.001	Test
C-ISS-01080	IR1	The ISS shall reuse the V0 WAN in order to provide connectivity between V0 network nodes and V1 network nodes and to provide interoperability between the systems.	BC002.001	Test
C-ISS-01100	A   IR1	The ISS shall provide for connectivity with TSDIS in order to transfer TRMM data to the GSFC DAAC.	BC002.001	Test
C-ISS-02000	IR1	The ISS shall provide connection oriented transport services as specified by the TCP protocol referenced in RFC 793.	BC002.002	Demo
C-ISS-02010	A   IR1	The ISS shall provide the capability to filter packets based on the port/socket of the transport layer protocol.	BC002.002 BC002.003	Demo
C-ISS-02020	A   IR1	The ISS shall provide connectionless transport services as specified by the UDP protocol referenced in RFC 768.	BC002.002	Demo / Inspect
C-ISS-02030	A   IR1	The ISS shall provide network layer services as specified by the Internet Protocol (IP) suite referenced in RFC 791.	BC002.002	Demo / Inspect
C-ISS-02050	A   IR1	The ISS shall provide ICMP network layer service as specified by RFC 792.	BC002.002	Demo / Inspect

req_source_id	release	text	test_id	Verif_Method
C-ISS-02060	IR1	The ISS shall provide network layer services in compliance with one or more of the following protocols as appropriate to the type of the physical network supported. a. IP over Ethernet as specified in RFCs 894, 895, 826 (ARP), 903 (RARP) b. IP over FDDI as specified in RFC 1188, 1390 (ARP, RARP) c. IP over HiPPI as specified in RFC 1374 (includes ARP, RARP) d. IP over SMDS as specified in RFC 1209 (includes ARP, RARP)	BC002.002	Demo / Inspect
C-ISS-02520	A   IR1	The ISS shall provide services based on the Open Shortest Path First (OSPF) protocol referenced in RFC 1583 to route traffic between the source and destination nodes, maintain route databases, and exchange routing information between networks.	BC002.002	Demo / Inspect
C-ISS-02530	A   IR1	The ISS shall provide services based on the Routing Information Protocol (RIP) referenced in RFC 1058 to route network traffic between the source and destination nodes.	BC002.002	Demo / Inspect
C-MSS-10060	IR1	The MSS shall interface with the Tropical Rainfall Measuring Mission (TRMM) to exchange data identified in Table 5.1-1 as specified in ECS/TRMM IRD, 194-219-SE1-018.	TC001.001	Test
C-MSS-10080	IR1	The MSS shall interface with the NASA Science Internet (NSI) to exchange data identified in Table 5.1-1 as specified in ECS/NSI IRD, 194-219-SE1-001.	TC001.001	Test
C-MSS-10410	A   IR1	The MSS shall interface with the CSS subsystems to exchange the data items in Table 5.1-5 as specified in the ECS internal ICDs, 313-DV3-003.	TC011.001 TC011.002	Test
C-MSS-12005	IR1	The MSS Management User Interface (MUI) Service shall be compatible with the ECS management framework.	TC014.004	Demo
C-MSS-12010	A   IR1	The MSS Management User Interface (MUI) Service shall provide a graphical user interface that is OSF/MOTIF compliant	TC014.004	Demo
C-MSS-12020	A   IR1	The MSS MUI Service shall have the capability to respond to keyboard and mouse input devices	TC014.004	Demo

req_source_id	release	text	test_id	Verif_Method
C-MSS-12030	IR1	The MSS MUI Service shall provide a capability for the M&O Staff to add/delete a symbol and to modify a symbol's shape, color and position	TC014.004	Demo
C-MSS-12040	IR1	The MSS MUI Service shall provide a capability for an application to add/delete a symbol and to modify a symbol's shape, color and position	TC014.004	Demo
C-MSS-12050	IR1	The MSS MUI Service shall provide a capability for the M&O Staff to add, delete, and modify text strings	TC014.004	Demo
C-MSS-12060	IR1	The MSS MUI Service shall provide a capability for an application to add, delete, and modify text strings	TC014.004	Demo
C-MSS-12070	IR1	The MSS MUI Service shall have the capability to provide options and methods to the M&O Staff for screen configuration changes (color, symbol placement, etc) and for retaining the changes from session to session	TC014.004	Demo
C-MSS-12080	A   IR1	The MSS MUI Service shall provide a capability for an applications to alert the M&O Staff	BC002.004 TC014.004	Demo
C-MSS-12090	A   IR1	The MSS MUI Service shall provide a capability for an applications to establish a dialog session with the M&O Staff	TC014.004	Demo
C-MSS-12100	IR1	The MSS MUI Service shall provide a capability for the M&O Staff to load and unload vendor or ECS defined MIB.	TC014.004	Demo
C-MSS-12110	IR1	The MSS MUI Service shall provide a capability for an applications to load and unload vendor or ECS defined MIB.	TC014.004	Demo
C-MSS-12120	IR1	The MSS MUI Service shall provide a capability for the operator to browse MIB values.	TC014.004	Demo
C-MSS-12130	IR1	The MSS MUI Service shall provide the capability for the M&O Staff to register and unregister managed objects.	TC014.004	Demo
C-MSS-12140	IR1	The MSS MUI Service shall provide the capability for an application to register and unregister managed objects.	TC014.004	Demo
C-MSS-12180	IR1	The MSS MUI Service shall provide the capability for an application to display on-line help windows	TC014.004	Demo

req_source_id	release	text	test_id	Verif_Method
C-MSS-14010	IR1	The MSS Maps/Collection Service shall retain the status of managed objects and their relationship to symbols that comprise a graphical representation of the physical network topology.	TC014.001	Demo
C-MSS-14020	A   IR1	The MSS Map/Collection Service shall provide a capability to define maps and objects.	TC014.001	Demo
C-MSS-14030	IR1	The MSS Map/Collection Service shall provide a capability to define a hierarchical relationship between maps and sub-maps (i.e., a graphical hierarchical tree)	TC014.001	Demo
C-MSS-14040	IR1	The MSS Map/Collection Service shall propagate events associated with objects up the hierarchical tree	TC014.001	Demo
C-MSS-16005	IR1	The ECS management protocol shall be the SNMP standard as specified in RFC 1157.	TC014.001	Demo / Inspect
C-MSS-16020	IR1	The MSS Monitor/Control Service shall communicate via ECS management protocol with the MSS Management Agent Service to request management data on a managed object.	TC014.003	Demo
C-MSS-16030	IR1	The MSS Monitor/Control Service shall be able to communicate via ECS management protocol with the MSS Management Agent Service to send ECS management set messages to configure and control the processing performed by the ECS management agent.	TC014.006	Demo
C-MSS-16040	IR1	The MSS Monitor/Control Service shall communicate via ECS management protocol with the MSS Management Agent Service to receive ECS management traps/events.	BC002.004 TC014.006	Demo
C-MSS-16050	IR1	The MSS Monitor/Control Service shall allow customized M&O staff-event notifications and automatic actions.	BC016.001 TC014.002	Demo
C-MSS-16060	IR1	The MSS Monitor/Control Service shall allow the capability to set thresholds on managed resources that are monitored	TC014.001	Demo
C-MSS-16070	IR1	The MSS Monitor/Control Service shall automatically report when a threshold has been exceeded by generating a ECS management event	BC002.004 TC014.001	Demo

req_source_id	release	text	test_id	Verif_Method
C-MSS-16100	IR1	The MSS Monitor/Control Service shall perform the following protocol test on managed network nodes: a. IP test b. TCP test c. SNMP test d. UDP test e. ICMP test	TC014.001	Demo
C-MSS-20010	IR1	The MSS Discovery Service shall discover (via network protocol) new instances of managed objects.	TC014.001	Demo
C-MSS-20020	IR1	The MSS Discovery Service shall detect missing occurrences of managed objects.	TC014.001	Demo
C-MSS-20030	IR1	The MSS Discovery Service shall report missing occurrences of managed objects.	TC014.001	Demo
C-MSS-20040	IR1	The MSS Discovery Service shall update the object database after the Discovery Service receives a request to register/unregister a managed object.	TC014.001	Demo
C-MSS-36010	IR1	The MSS Management Agent Service shall retrieve data from ECS managed objects in test or operational mode.	TC014.003	Demo
C-MSS-36020	IR1	The MSS Management Agent Service shall communicate via ECS management protocol with the MSS Monitor/Control Service to respond to requests for managed object MIB attributes	TC014.006	Demo
C-MSS-36040	IR1	The MSS Management Agent Service shall communicate via ECS management protocol with the MSS Monitor/Control Service to send ECS management traps/events to the Monitor/Control Service.	TC014.006	Demo
C-MSS-36050	IR1	The MSS Management Agent Service shall communicate via ECS management protocol with the MSS Monitor/Control Service to receive ECS management set message from the Monitor/Control Service.	TC014.006	Demo
C-MSS-36060	IR1	The MSS Management Agent Service shall provide an ECS management agent that is configurable to include: a. Community to respond to and set attributes b. Agent location & contact person c. Traps to send d. Events to log & log file name	TC014.006	Demo

req_source_id	release	text	test_id	Verif_Method
C-MSS-36070	A   IR1	The MSS Management Agent Service shall provide an ECS management agent for network devices	TC014.006	Demo
C-MSS-40400	A   IR1	The MSS configuration management application service at the sites and the SMC shall maintain software libraries to store files containing versions and platform variants of: <ul style="list-style-type: none"> <li>a. source code;</li> <li>b. binaries and executables;</li> <li>c. patches;</li> <li>d. calibration coefficients and control data;</li> <li>e. scripts;</li> <li>f. designs and design specifications;</li> <li>g. databases;</li> <li>h. technical documentation (both text and graphics);</li> <li>i. test data;</li> <li>j. test reports;</li> <li>k. interface specifications;</li> <li>l. configuration data. (IR-1)</li> </ul>	Verified in AI&T test cases upon consolidation of three test plans	Demo
C-MSS-40410	A   IR1	The MSS configuration management application service at each DAAC shall maintain user-definable software configuration status information for each algorithm. (IR-1)	Verified in AI&T test cases upon consolidation of three test plans	Demo
C-MSS-40420	A   IR1	The MSS configuration management application service at each site shall maintain M&O staff-definable software configuration status information for each version of every software library file.	Verified in AI&T test cases upon consolidation of three test plans	Demo
C-MSS-40470	A   IR1	The MSS configuration management application service shall regulate operations on software library files through use of individual and group permissions.	Verified in AI&T test cases upon consolidation of three test plans	Demo
C-MSS-40480	A   IR1	The MSS configuration management application service shall use a checkout/edit/checkin paradigm to govern changing of software library files.	Verified in AI&T test cases upon consolidation of three test plans	Demo

req_source_id	release	text	test_id	Verif_Method
C-MSS-40490	A   IR1	The MSS configuration management application service shall track each software library file that has been changed as a new version of the original file.	Verified in AI&T test cases upon consolidation of three test plans	Demo
C-MSS-40500	A   IR1	The MSS configuration management application service shall merge versions of software library files and identify version conflicts, if any.	Verified in AI&T test cases upon consolidation of three test plans	Demo
C-MSS-40510	A   IR1	The MSS configuration management application service shall maintain records of actual changes made to ECS software library files in implementing system enhancement requests.	Verified in AI&T test cases upon consolidation of three test plans	Demo
C-MSS-40520	A   IR1	The MSS configuration management application service shall verify that changes to software library files are supported by approved change requests.	Verified in AI&T test cases upon consolidation of three test plans	Demo
C-MSS-40540	A   IR1	The MSS configuration management application service shall perform builds of baseline systems for ECS platforms and audit the builds such that they can be repeated.	Verified in AI&T test cases upon consolidation of three test plans	Demo
C-MSS-40550	A   IR1	The MSS configuration management application service shall reconstruct previous versions of software library files.	Verified in AI&T test cases upon consolidation of three test plans	Demo
C-MSS-40560	A   IR1	The MSS configuration management application service shall allow concurrent user access to software library files.	Verified in AI&T test cases upon consolidation of three test plans	Demo
C-MSS-40570	A   IR1	The MSS configuration management application service shall maintain an audit trail of all changes made to software library files.	Verified in AI&T test cases upon consolidation of three test plans	Demo

req_source_id	release	text	test_id	Verif_Method
C-MSS-40990	A   IR1	The MSS configuration management application service shall log the following information for configuration management events: a. operation type; b. userid of initiator; c. date-time stamp; d. host name. (IR-1, at the sites only)	Verified in AI&T test cases upon consolidation of three test plans	Demo
C-MSS-40995	A   IR1	The MSS configuration management application service shall generate chronological reports of logged CM events associated with M&O staff-selectable: a. time frames; b. operation types; c. userids; d. hosts.	Verified in AI&T test cases upon consolidation of three test plans	Demo
C-MSS-60010	A   IR1	The MSS Fault Management Application Service shall provide the capability to create and display graphical representations of a given network topology consisting of the following: a. routers b. communication lines c. hosts d. peripherals e. applications	TC014.001	Demo
C-MSS-60020	A   IR1	The MSS Fault Management Application Service shall provide the capability to define categories of faults.	TC014.003	Demo
C-MSS-60080	A   IR1	The MSS Fault Management Application Service shall have the capability to establish, view, modify and delete thresholds on performance metrics it measures.	TC013.005	Demo
C-MSS-60100	A   IR1	The MSS Fault Management Application Service shall have the capability to poll for the detection of fault/performance information.	TC014.003	Demo
C-MSS-60110	A   IR1	The MSS Fault Management Application Service shall be capable of receiving fault notifications.	BC002.004	Demo
C-MSS-60120	A   IR1	The MSS Fault Management Application Service shall have the capability to define the frequency with which polling is done for the detection of fault/performance information.	TC014.003	Demo

req_source_id	release	text	test_id	Verif_Method
C-MSS-60130	IR1	<p>The MSS Fault Management Application Service shall provide the capability to detect the following types of faults, errors and events:</p> <ul style="list-style-type: none"> <li>a. communications software version mismatch errors</li> <li>b. communication software configuration errors</li> <li>c. the following errors in communication hardware: <ul style="list-style-type: none"> <li>1. host not reachable</li> <li>2. router not reachable</li> <li>3. errors and failures of communication links</li> </ul> </li> <li>d. Errors in the communications protocols supported</li> <li>e. degradation of performance due to established thresholds being exceeded</li> <li>f. Peripherals</li> <li>g. Databases</li> <li>h. Applications: <ul style="list-style-type: none"> <li>1. process missing (Application or COTS product)</li> <li>2. process in a loop</li> <li>3. process failed</li> </ul> </li> </ul>	BC002.004	Demo
C-MSS-60140	A   IR1	The MSS Site Fault Management Application Service shall have the capability to generate a fault notification when a predefined threshold on a performance metric is exceeded.	BC002.004	Demo
C-MSS-60150	A   IR1	The MSS Fault Management Application Service shall have the capability to receive fault notifications from the Management Agent Service.	BC002.004	Demo
C-MSS-60170	A   IR1	<p>The MSS EMC Fault Management Application Service shall be capable of requesting fault notification and performance degradation data from :</p> <ul style="list-style-type: none"> <li>a. Site Fault Management Applications</li> <li>b. Other external systems as defined in Section 5.1.</li> </ul>	BC002.004	Demo
C-MSS-60190	A   IR1	The MSS Fault Management Application Service shall use the Logging Services to record each detected fault.	TC013.003 TC013.004	Test

req_source_id	release	text	test_id	Verif_Method
C-MSS-60200	A   IR1	<p>The MSS Fault Management Application Service shall have the capability to generate the following types of notifications for detected faults :</p> <ul style="list-style-type: none"> <li>a. a change in the color of an icon on a display</li> <li>b. a message in a pop-up notification window</li> <li>c. logging the following fault information to a disk log file: <ul style="list-style-type: none"> <li>1. fault type</li> <li>2. date and time of occurrence of the fault</li> <li>3. identification of the source of the notification (e.g. IP address, process name, etc.)</li> <li>4. fault data received with the notification</li> <li>5. operator-defined descriptive text</li> </ul> </li> <li>d. audible alert</li> </ul>	BC002.004	Demo
C-MSS-60310	IR1	<p>The MSS Fault Management Application Service shall provide utilities to perform diagnostics and testing of the following for the purpose of fault isolation:</p> <ul style="list-style-type: none"> <li>a. connectivity between pairs of ECS hosts and ECS routers</li> <li>b. ability to reach hosts and routers</li> <li>c. availability of network services at hosts</li> </ul>	BC002.004	Demo
C-MSS-60340	A   IR1	The MSS Fault Management Application Service shall be capable of verifying the operational status of a host.	BC002.004	Demo
C-MSS-60370	A   IR1	<p>The MSS Fault Management Application Service at the SMC shall be capable of sending gathered isolation, location, identification and characterization of reported faults data to the level of subsystem and equipment to the following:</p> <ul style="list-style-type: none"> <li>a. the site Fault Management Applications</li> <li>b. other external systems as defined in Section 5.1.</li> </ul>	TC014.001 TC014.005	Demo

req_source_id	release	text	test_id	Verif_Method
C-MSS-60380	IR1	The MSS Fault Management Application Service at the sites shall isolate, locate, and identify faults, identify subsystem, equipment and software faults, and identify the nature of the faults detected within its site.	TC014.002	Demo
C-MSS-60500	A   IR1	The MSS EMC Fault Management Application Service shall coordinate the recovery from conditions of performance degradation and faults with the sites and external network service providers.		Demo
C-MSS-60600	IR1	The MSS Fault Management Application Service shall have the capability to generate, on an interactive and on a scheduled basis, reports on performance/error data that it has been configured to collect.	TC014.001 TC014.005	Demo
C-MSS-60620	A   IR1	The MSS Fault Management Application Service shall have the capability to redirect reports to: a. console b. disk file c. printer	TC014.001 TC014.005	Demo
C-MSS-66000	IR1	The MSS performance management application service shall be capable of monitoring the performance of the following ECS components a. network components 1. routers 2. links 3. bridges 4. gateways	TC014.001	Demo
C-MSS-66010	A   IR1	The MSS performance management application service shall be capable of monitoring ECS component protocol stack performance parameters defined in IETF RFC 1213.	TC014.001	Demo / Inspect
C-MSS-66020	IR1	The MSS Performance Management Application Service shall be capable of monitoring ethernet-like device performance parameters as specified in IETF RFC 1623.	TC014.001	Demo / Inspect
C-MSS-66030	A   IR1	The MSS performance management application service shall be capable of receiving managed object definitions for each managed object.	TC014.005	Demo

req_source_id	release	text	test_id	Verif_Method
C-MSS-66040	IR1	The MSS performance management application service shall be capable of specifying which available performance metrics are to be gathered from each individual managed object.	TC014.005	Demo
C-MSS-66040	A   IR1	The MSS performance management application service shall be capable of specifying which available performance metrics are to be gathered from each individual managed object.	TC014.005	Demo
C-MSS-66050	IR1	The MSS performance management application service shall be capable of requesting performance data from each individual managed object: a. at configurable intervals b. on demand.	TC014.005	Demo
C-MSS-66060	IR1	The MSS performance management application service shall be capable of receiving requested performance data from ECS components.	TC014.005	Demo
C-MSS-66080	A   IR1	The MSS performance management application service shall be capable of retrieving the following data for all network component interfaces: a. operational status b. type c. speed d. octets in/out e. packets in/out f. discards in/out g. errors in/out	TC014.005	Demo
C-MSS-66080	IR1	The MSS performance management application service shall be capable of retrieving the following data for all network component interfaces: a. operational status b. type c. speed d. octets in/out e. packets in/out f. discards in/out g. errors in/out	TC014.005	Demo

req_source_id	release	text	test_id	Verif_Method
C-MSS-66100	IR1	The MSS performance management application service shall be capable of retrieving the following data for all hosts: a. total CPU utilization b. memory utilization c. physical disk i/o's d. disk storage size e. disk storage used f. number of active processes g. length of run queue h. network i/o's (packets) i. network errors	TC014.005	Demo
C-MSS-66120	IR1	The MSS performance management application service shall be capable of determining the operational state of all network components, hosts, and peripherals to be: a. on-line b. off-line c. in test mode	TC014.001	Demo
C-MSS-66130	IR1	The MSS performance management application service shall be capable of receiving operational state change notifications from network components, hosts, applications, and peripherals.	TC014.001	Demo
C-MSS-66170	A   IR1	The MSS performance management application service shall log ECS performance data pertaining to ECS network components and operating system resources.	TC014.001	Demo
C-MSS-66180	A   IR1	The MSS performance management application service shall have the capability to generate the following types of statistics for a configurable period of time for performance data stored in the Management Database: a. average b. median c. maximum d. minimum e. ratios f. rates g. standard deviations.	TC013.003	Demo
C-MSS-66190	A   IR1	The MSS performance management application service shall provide a configurable number of thresholds for each performance metric.	TC013.005	Demo

req_source_id	release	text	test_id	Verif_Method
C-MSS-66200	A   IR1	The MSS EMC performance management application service shall be capable of creating a list of suggested initial threshold values for each performance metric.	TC013.005	Demo
C-MSS-66230	IR1	The MSS performance management application service shall allow each performance metric threshold to be configurable.	TC013.005	Demo
C-MSS-66240	IR1	The MSS performance management application service shall be capable of evaluating each performance metric against defined thresholds.	TC013.005	Demo
C-MSS-66250	IR1	The MSS performance management application service shall record an event in the local History Log whenever a threshold is crossed.	TC013.003	Test
C-MSS-66260	A   IR1	The MSS performance management application service shall provide queries that generate performance statistics from performance data stored in the Management Database.	TC013.003	Demo
C-MSS-66270	A   IR1	The MSS performance management application service shall store generated performance statistics.	TC013.003	Demo
C-MSS-66310	IR1	The MSS performance management application service shall be capable of retrieving the following science algorithm performance data via the Management Data Access Service: a. algorithm name b. algorithm version c. start time d. stop time e. CPU utilization f. memory utilization g. disk reads h. disk writes	TC013.003	Test
C-MSS-68000	A   IR1	The MSS performance management application service shall be capable of graphically displaying the operational state of managed objects through the MUI service.	TC014.004	Demo

req_source_id	release	text	test_id	Verif_Method
C-MSS-68010	A   IR1	The MSS performance management application service shall be capable of displaying M&O staff-selected performance statistics through the MUI in tabular and graphical formats.	TC014.004	Demo
C-MSS-68020	A   IR1	The MSS performance management application service shall be capable of printing M&O staff-selected performance statistics.	TC014.004	Demo
C-MSS-68100	A   IR1	The MSS Performance Management Application Service shall have the capability to redirect reports to: a. console b. disk file c. printer	TC014.001 TC014.005	Demo
C-MSS-70010	IR1	The MSS Security Management Application Service shall provide the capability to create, modify and delete user accounts with the following attributes: a. username b. password c. group identification code d. user identification code e. login directory f. command line interpreter	TC003.005	Demo
C-MSS-70020	IR1	The MSS Security Management Application Service shall enable the assignment of user accounts to groups based on the group identification code.	TC003.005	Demo
C-MSS-70100	A   IR1	The MSS site Security Management Application Service shall provide the capability to set, maintain, and update access control information for ECS resources.	TC003.005	Demo
C-MSS-70120	IR1	The MSS site Security Management Application service shall provide the mechanism, for each ECS host, to allow or deny incoming requests from specific hosts to services.	TC003.002 TC003.003 TC003.004 TC003.005 TC003.006	Demo
C-MSS-70130	A   IR1	The MSS site Security Management Application Service shall provide a command line interface and a GUI for the management of the following security databases: a. Authentication Database b. Authorization Database c. Network Database	TC003.001 TC003.005	Demo

req_source_id	release	text	test_id	Verif_Method
C-MSS-70300	A   IR1	The MSS site Security Management Application Service shall have the capability to perform the following types of security tests: a. password auditing b. file system integrity checking c. auditing of user privileges d. auditing of resource access control information	TC003.001 TC003.005	Demo
C-MSS-70520	IR1	The MSS EMC Security Management Application Service shall provide office automation support tools to enable the generation of directives and instructions for recovery from detected security events.		Demo
C-MSS-70700	A   IR1	The MSS Security Management Application Service shall have the capability to generate intrusion reports on the following: a. Login failures b. Unauthorized access to ECS resources c. Break-ins d. Viruses and worms	TC003.005	Test
C-MSS-70710	IR1	The MSS Security Management Application Service shall have the capability to generate reports from collected management data.	TC003.005	Demo
C-MSS-70720	A   IR1	The MSS Security Management Application Service shall have the capability to redirect reports to: a. console b. disk file c. printer	TC014.001 TC014.005	Demo
C-MSS-90150	A   IR1	The DBMS shall support access structures (i.e., single-level indexes, multilevel indexes) to improve the efficiency of retrieval of management data.	TC013.003	Demo
C-MSS-90570	A   IR1	The Report Generator shall have the capability to generate charts and graphs (e.g., bar, pie, line, etc.) from management data maintained in the DBMS.	TC013.003	Demo

req_source_id	release	text	test_id	Verif_Method
C-MSS-91020	IR1	The MSS Office Automation shall provide a spreadsheet capability that: a. simulates and displays an accountant's worksheet b. enables revisions and calculations on the displayed worksheet's data c. enables transfer of the worksheet data to database, word processing and graphics applications d. enables printing of worksheet information.	TC0013.003 TC0014.005	Demo
No Explicit Requirements - DCE Ticket Expiration			TC003.008	Demo
No Explicit Requirements - Basic Demo of DCE DNS			TC004.001	Demo
No Explicit Requirements - Basic Demo of DCE DNS			TC004.002	Demo
No Explicit Requirements - Basic Demo of DCE DNS			TC004.003	Demo
No Explicit Requirements - Basic Demo of DCE DTS			TC005.001	Demo
No Explicit Requirements - Basic Demo of DCE DTS			TC005.002	Demo
No Explicit Requirements - Basic Demo of DCE DTS			TC005.003	Demo
No Explicit Requirements - Basic Demo of DCE DTS			TC005.004	Demo

<b>req_source_id</b>	<b>release</b>	<b>text</b>	<b>test_id</b>	<b>Verif_Method</b>
No Explicit Requirements - Basic Demo of DCE DTS			TC005.005	Demo
No Explicit Requirements - Basic Demo of DCE (General)			BC008.001	Demo

This page intentionally left blank.

# Abbreviations and Acronyms

---

ACL	access control list
AI&T	Algorithm Integration and Test
API	Application Programmer Interface
BBS	bulletin board server
CCR	configuration change request
CDR	Critical Design Review
CDRL	contract data requirements list
CDS	Cell Directory Service
CDSCP	cell directory service command program
CERES	Clouds and Earth's Radiant Energy System
CI	configuration item
CM	configuration management
CMAS	Configuration Management Application Service
COTS	commercial off-the-shelf
CSC	computer software component
CSCI	computer software configuration item
CSMS	Communications and Systems Management Segment
CSR	Consent to Ship Review
CSS	Communications SubSystem
CSU	computer software unit
DAAC	Distributed Active Archive Center
DBMS	Data Base Management System
DCCI	Distributed Computing CI
DCE	Distributed Computing Environment
DCHCI	Distributed Computing Hardware CI
DCN	document change notice
DDTS	Distributed Defect Tracking System
DFS	distributed file service

DID	data item description
DTS	distributed time service
DV1	document version 1
ECS	EOSDIS Core System
EDC	EROS Data Center (DAAC)
EDF	ECS Development Facility
EDHS	ECS Data Handling System
EOC	ECS Operations Center
EOS	Earth Observation System
EOSDIS	Earth Observation System Data Information System
EP	Evaluation Package
EROS	Earth Resources Observation System
ESN	EOSDIS Science Network
ETR	Element Test Review
FDF	flight dynamics facility
F&PRS	Functional and Performance Requirements Specifications
FOS	Flight Operations Segment
FTP	file transfer protocol
GDS	Global Directory Service
GSFC	Goddard Space Flight Center
HWCI	Hardware CI
I&T	Integration and Test
IATO	Independent Acceptance Test Organization
ICD	Interface Control Document
IDL	interactive data language
IDR	internal design review
INCI	Internetworking CI
INHCI	Internetworking Hardware CI
IP	Internet protocol
IR-1	Interim Release one
ISO	International Standards Organization

ISS	Internetworking SubSystem
IV&V	Independent Verification and Validation
JPL	Jet Propulsion Laboratory
LAN	Local Area Network
LaRC	Langley Research Center
LIS	Lightning Imaging Sensor
M&O	Maintenance and Operations
MACI	Management Agent Software CI
MCI	Management Software CI
MG1	Management one
MHCI	Management Hardware CI
MIB	Management Information Base
MLCI	Management Logistics Software CI
MOC	Mission Operations Center
MSFC	Marshall Space Flight Center
MSS	Management SubSystem
MUI	Management User Interface
NASCOM	NASA Communications
NCR	Nonconformance Reporting
NOAA	National Oceanic and Atmospheric Administrator
NOLAN	NASCOM Operational Local Area Network
NRCA	Nonconformance Reporting And Corrective Action
NSI	NASA Science Internet
OODCE	Object Oriented DCE
OSI	Open System Interconnect
OSPF	Open Shortest Path First (routing protocol)
OSI-RM	OSI - Reference Model
PDR	preliminary design review
PGS	Product Generation System
PMAS	Performance Management Application Service
RFC	Request for Comment

RFP	Request for Proposal
RIP	Router Information Protocol
RPC	remote procedure call
RRR	Release Readiness Review
RTM	requirements traceability matrix
SCF	Science Computing Facility
SDPF	Science Data Processing Facility
SDPS	Science Data Processing Segment
SEI	Software Engineering Institute
TBD	to be determined
TCP	Transmission Control Protocol
TMI	TRMM Microwave Image
TRMM	Tropical Rainfall Measuring Mission (joint US-Japan
TRR	test readiness review
TSDIS	TRMM Science Data and Information System
UTC	universal time code
V0	Version Zero
VOB	Version Object Base